CLEANING-UP AFTER *CARPENTER*: PERSONAL DATA AS PROPERTY UNDER THE FOURTH AMENDMENT

Alessandra Masciandaro[*]

I. INTRODUCTION

"Changes in law [are] full of danger."[1] The Supreme Court's adherence to the principle of stare decisis speaks to this truth. Rather than leap to upend well-settled doctrine, when novel situations arise, the Court turns to legal fictions to achieve justice while applying existing law[2]—"[f]or the written word remains, but man changes."[3] Tensions rise when popular ideas of justice conflict with the written law.[4] To harmonize the two, legal fictions erupt that "mark where there was once a distinction between law in the books and law in action, and show one way in which the two have been brought into accord."[5] But the use of legal fictions is not without consequences.[6]

Today the United States is caught in the throes of a legal fiction developed to extend Fourth Amendment protection to objects of an individual's privacy—the *Katz* "reasonable expectation of privacy" test.[7]

[*]J.D. Candidate, 2021, Seton Hall University School of Law; B.A., with High Honors in Philosophy, 2007, Rutgers University. The author expresses her gratitude to Professor of Law and Co-Director of the Gibbons Institute of Law, Science & Technology David Opderbeck for the inspiration, guidance, and challenges that made this Comment possible. She also thanks Hannah Levine, Stephanie Torres, Mikayla Berliner, Antonio Vayas, and Nathan "Avi" Muller for their help refining this Comment.

[1] Roscoe Pound, *Law in Books and Law in Action*, 44 AM. L. REV. 12, 12 (1910).

[2] *See id.* at 12–13. Pound employs a metaphor, describing the practice of using legal fictions as the way "the law has always managed to get a pickaxe in its hands, though it steadfastly demanded a case-knife, and to wield it in the virtuous belief that it was using the approved instrument." *Id.*

[3] *Id.* at 36.

[4] *Id.* at 13–15 (presenting examples of legal fictions from archaic legal systems through the twentieth century).

[5] *Id.* at 14.

[6] *See infra* Part V.

[7] *See generally* Katz v. United States, 389 U.S. 347 (1967) (holding that a conversation that the defendant had while within a phonebooth was protected under the Fourth Amendment because he had a "reasonable expectation of privacy"—a new standard for Fourth Amendment protection).

Examining the history of the Fourth Amendment[8] and the line of jurisprudence that follows from *Katz*[9] reveals a sharp divide between the original intent of the Fourth Amendment and its actual application today. While courts have perpetuated the use of the *Katz* test, it stands on shaky ground.[10]

In 2018, the Supreme Court decided *Carpenter v. United States* by applying *Katz*'s reasonable expectation of privacy test.[11] The Court found that law enforcement officers had violated Carpenter's right to be free from unreasonable search and seizure when those officers accessed Carpenter's historic cell-site location information without a warrant because Carpenter had a reasonable expectation of privacy in the whole of his movements.[12] Despite the Court's presumably good intentions, this holding has left lower courts struggling to properly apply the Fourth Amendment to other forms of personal data.[13]

In its essence, the difficulty that *Carpenter* created appears to stem from applying two legal fictions to protect location data: (1) the *Katz* test; and (2) the premise that privacy rights—not property rights—apply to personal data. The law as written and the sensibilities of the people diverge—the law on the books says that the Fourth Amendment only protects "persons, houses, papers, and effects," but the law in action says that it also protects reasonable expectations of privacy; the law on the books says only privacy rights extend to personal data, but the law in action says personal data is property.[14]

---

[8] *Infra* Section III.A.

[9] *Infra* Section III.B.

[10] Trevor Burrus & James Knight, Katz *Nipped and* Katz *Cradled:* Carpenter *and the Evolving Fourth Amendment*, 2017 CATO SUP. CT. REV. 79, 110 (2017–2018).

[11] Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018) (5-4 decision).

[12] *Id.* at 2219.

[13] *See* Allison Grande, *Location Privacy Warrant Lines Still Murky After Carpenter*, LAW360 (Aug. 19, 2019), https://www.law360.com/articles/1189523 ("[T]he [C]ourt left open whether the requirement applies to other categories of sensitive digital data, such as real-time cellphone records, internet browsing histories, toll transactions and smart meter usage.").

[14] American legislatures have not explicitly granted property-status to personal data; however, state legislatures are increasingly treating personal data as property under data privacy laws. *See, e.g.*, Illinois Biometric Information Privacy Act of 2008, 740 ILL. COMP. STAT. 14 (2008) (allowing for a cause of action even where no actual injury occurred—a violation of statutory protection of biometric information alone suffices to establish standing); California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–1798.199 (West 2020) (granting individuals the right to have their personal information deleted).

Legal fictions "soon get into the books and become part of the law as it is written."[15] This Comment analyzes the implications of classifying personal data as property under the Fourth Amendment. Doing so could relieve the judicial system of the confusion caused by applying two legal fictions to personal data under the Fourth Amendment. Law enforcement could benefit from a categorical rule as to when a warrant is required. Recognizing personal data as property under the Fourth Amendment could also benefit individuals by ensuring that the Fourth Amendment will protect their personal data from unreasonable search and seizure.

The expansion of state data privacy laws provides a basis that could allow the Supreme Court to find that state legislatures have implicitly recognized a property right in personal data; as such, when an appropriate case or controversy arises, the Court could hold that personal data is property that the Fourth Amendment protects. Employing legal fictions—the reasonable expectation of privacy test[16] and classifying personal data as an object of privacy rights alone—would no longer be necessary to apply the Fourth Amendment to personal data. In theory, this could allow for predictable warrant requirements and a consistent administration of justice. But personal data is complex. Issues arise as to its proper definition and to whom data should belong.[17]

This Comment examines the possibility that personal data could be brought under the Fourth Amendment as a form of property. Part II of this Comment analyzes the Court's decision in *Carpenter* and discusses the difficulties that this decision has created. Part III explores the text and history surrounding the adoption of the Fourth Amendment. It then provides an overview of *Katz* and its progeny leading up to the Court's decision in *Carpenter*. In Part IV, this Comment explores how current and pending state data privacy legislation treat personal data as property. This Part also explores various definitions of personal data and their implications for this analysis. Part V considers whether recognizing personal data as property under the Fourth Amendment would heighten courts' efficiency in applying the Fourth Amendment to

---

15 Pound, *supra* note 1, at 14.

16 *See generally* Katz v. United States, 389 U.S. 347 (1967) (setting forth the reasonable expectation of privacy test).

17 *See* Andy Green, *Complete Guide to Privacy Laws in the US*, VARONIS (Mar. 29, 2020), https://www.varonis.com/blog/us-privacy-laws (comparing various definitions of personal information under proposed state data privacy laws); *see also* Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. REV. 423, 463 (2018) (describing the question of data ownership or rights as a "vexing" question in the context of Internet of Things devices).

personal data. This Part also explores the difficulty in defining "personal data" as property, given longstanding notions of the appropriate objects of property rights. In Part VI, this Comment discusses consequences that may follow if state legislatures widely adopted the notion that personal data is property. This Comment suggests that the states should continue to cautiously exercise their roles as laboratories, imparting piecemeal property rights to personal data and evaluating their impact. Part VII concludes that while a Supreme Court opinion holding that personal data is property under the Fourth Amendment could eliminate the need to resort to legal fictions in this context, the difficulties in defining which items of "personal data" qualify as property may leave courts no better off than using the *Katz* test.

II. *CARPENTER*'S CONTROVERSIAL PROTECTION OF HISTORIC CELL-SITE LOCATION INFORMATION

In *United States v. Carpenter*, the Supreme Court divided on whether historic cell-site location information falls under the Fourth Amendment.[18] The majority ruled that it does because individuals have a reasonable expectation of privacy in the whole of their physical movements.[19] Four dissenters each authored separate opinions. Despite this divide among the dissenters, each invoked the concept of applying the Fourth Amendment to property interests. If the Court recognized personal data as an effect belonging to the person to whom it pertains, the Court might have unanimously agreed that historic cell-site location information is subject to the Fourth Amendment. An analysis of each opinion follows.

A. *The Majority Opinion*

The majority of the Supreme Court concluded that acquiring a historic record of an individual's movements over an extended period constitutes a Fourth Amendment search.[20] This result was foreshadowed by dicta in *United States v. Jones*.[21] At first, the *Carpenter* decision appeared to bring important Fourth Amendment protection to individuals in the modern-day era, but this impression quickly faded as

[18] 138 S. Ct. 2206, 2211 (2018).
[19] *Id.* at 2219.
[20] *Id.*
[21] 565 U.S. 400, 430 (2012).

courts demonstrated a reluctance to require a warrant for access to similar records.[22]

The Court applied *Katz*'s reasonable expectation of privacy test to cell-site location information (CSLI), which revealed "the whole of [Carpenter's] physical movements."[23] Additionally, the Court examined the nature of CSLI acquisition under a multifactor analysis that it had previously used to evaluate "such surveillance techniques as bugging, wiretaps, video surveillance, and email acquisitions" under the Fourth Amendment.[24] When law enforcement officers acquired Carpenter's CSLI, they accessed the whole of his physical movements in a hidden, continuous, indiscriminate, and intrusive manner.[25] The Court found this method to be problematic because accessing CSLI provides a "near perfect" surveillance.[26] By grasping onto *Katz*'s reasonable expectation of privacy test and supplementing its analysis by considering problematic surveillance methods, the Court managed to bring historic CSLI under the Fourth Amendment.

This feat of judicial gymnastics ultimately achieved an outcome that many would regard as just, but it failed to provide an intelligible precedent for lower courts to follow.[27] Essentially, the Court treated personal data as property by bringing it within the scope of the Fourth Amendment—a provision of our Constitution designed to protect persons, their houses, and their intimate personal property.[28] Simply recognizing personal data as a form of property could have achieved the same result in an efficient and doctrinally sound manner if the Court were to take an agreeable approach to personal data.

---

[22] *See*, *e.g.*, Rick Aldrich, *Privacy's "Third-Party" Doctrine: Initial Developments in the Wake of* Carpenter, 15 SCITECH LAW. 4, 6–7 (2019) (stating that most decisions that cite *Carpenter*'s holding do not suppress CSLI evidence); *see also* Grande, *supra* note 13.

[23] *Carpenter*, 138 S.Ct. at 2219.

[24] Susan Freiwald & Stephen Wm. Smith, *The* Carpenter *Chronicle: A Near Perfect Surveillance*, 132 HARV. L. REV. 205, 219 (2018).

[25] *See id.* at 221.

[26] *Id.*

[27] *See*, *e.g.*, Aldrich, *supra* note 22, at 6–7 (stating that most decisions that cite *Carpenter*'s holding do not suppress CSLI evidence); *see also* Grande, *supra* note 13.

[28] *See Carpenter*, 138 S. Ct. at 2255 (Alito, J., dissenting) ("For the majority, this case is apparently no different from one in which Government agents raided Carpenter's home and removed records associated with his cell phone."). The third-party doctrine provides that individuals do not possess a reasonable expectation of privacy in anything disclosed to a third party.

In *Smith v. Maryland*[29] and *United States v. Miller*,[30] the government attempted to justify its warrantless access of Carpenter's CSLI by turning to the third-party doctrine.[31] This argument failed.[32] The Court found that the third-party doctrine was ill-suited to handle "the exhaustive chronicle of location information casually collected by wireless carriers today."[33] While *Smith* and *Miller* address "limited types of personal information," CSLI provides a comprehensive chronicle of personal information that implicates significantly greater privacy concerns.[34] Further, the Court found that CSLI is not transmitted voluntarily.[35] Rather, wireless providers automatically collect CSLI whenever a cell phone is connected to their network.[36]

Carpenter limited the third-party doctrine, finding that it does not apply to CSLI because of the detailed, chronological nature of CSLI and the involuntary manner in which it is collected.[37] Scholars suggest that this holding indicates that a warrant should be required when an individual's "reasonable expectation of privacy in the records converts the records into the modern-day equivalent of an individual's own papers or effects . . . whether [or not] those records are stored with . . . a third party."[38] While this suggestion achieves the desired result of avoiding the third-party doctrine, it suggests a complicated procedure to do so. Rather than first debating whether a person has a reasonable expectation of privacy in their records, personal data could be categorically recognized as an "effect." This would impose a warrant requirement on personal data, eliminating normative judgments about which expectations of privacy are reasonable.

---

29 442 U.S. 735 (1979).

30 425 U.S. 435 (1976).

31 *Carpenter*, 138 S. Ct. at 2219.

32 *Id.*

33 *Id.*

34 *Id.* at 2219–20.

35 *Id.* at 2220 ("Cell phone location information is not truly 'shared' as one normally understands the term.").

36 *Id.*

37 *Carpenter*, 138 S. Ct. at 2219–20; *see also* Freiwald & Smith, *supra* note 24, at 218 ("[T]he majority found that cell site records, due to their unique and revealing nature, were not subject to the third party doctrine of *Smith* and *Miller*.").

38 Freiwald & Smith, *supra* note 24, at 226.

B. *The Dissenting Opinions*

Carpenter presented a contentious issue, which resulted in a 5-4 split among the Justices.[39] Justices Kennedy, Thomas, Alito, and Gorsuch dissented.[40] Though each Justice made a distinct argument to reject the majority's decision, one common theme ran through each dissenting opinion—an emphasis on property concepts.[41]

Justice Kennedy's dissent, joined by Justices Thomas and Alito, rested on the premise that the third-party doctrine should apply to CSLI.[42] From Justice Kennedy's perspective, the issue should have been addressed "by interpreting accepted property principles as the baseline for reasonable expectations of privacy."[43] Since Carpenter's wireless provider created and retained the CSLI records, Justice Kennedy believed that the records should be regarded as the wireless provider's property; therefore, the third-party doctrine should insulate them from the Fourth Amendment.[44] Accordingly, acquiring CSLI records should then merely require a subpoena *duces tecum*.[45]

Justice Thomas carefully parsed the text of the Fourth Amendment in his dissenting opinion.[46] First, Justice Thomas drew attention to the word "their" from the phrase protecting individuals "from unreasonable searches of '*their* persons, houses, papers, and effects.'"[47] Carpenter must prove the CSLI is *his* in order to come under the Fourth Amendment.[48] This analysis stresses that "their" indicates that the key issue is "*whose* property was searched."[49] In addition to this assertion, Justice Thomas heavily criticizes *Katz*'s reasonable expectation of privacy test as inconsistent with a proper understanding of the Fourth Amendment.[50] Justice Thomas found that Carpenter's claim failed under an approach focused strictly on property concepts.[51] In his analysis, the Fourth Amendment's close connection to property presents itself

39 *Carpenter*, 138 S. Ct. 2206 (5-4 decision).

40 *Id.*

41 *See, e.g.*, *id.* at 2224, 2235, 2260 & 2268.

42 Freiwald & Smith, *supra* note 24 at 218.

43 *Carpenter*, 138 S. Ct. at 2235.

44 *Id.* at 2229–30.

45 *See id.* at 2235.

46 *Id.*

47 *Id.*

48 *Id.* at 2242.

49 *Carpenter*, 138 S. Ct. at 2235.

50 *Id.* at 2236 ("The more fundamental problem with the Court's opinion . . . is its use of the 'reasonable expectation of privacy' test . . . ."); Freiwald & Smith, *supra* note 24, at 218.

51 Freiwald & Smith, *supra* note 24, at 218.

through the text that limits protection to persons and "three specific types of property: 'houses, papers, and effects.'"[52] Since data is not recognized as one of these forms of property, Justice Thomas concluded the Fourth Amendment does not cover it.[53]

Justice Alito, joined by Justice Thomas, dissented on the basis that the government may use a subpoena to acquire CSLI, subject to relevance review.[54] From Justice Alito's perspective, the majority erred by expanding the protection against an unreasonable search of one's property to protect against an unreasonable search of a third party's property.[55] Justice Alito saw the majority's decision as fracturing two "fundamental pillars of Fourth Amendment law."[56] First, conflating the distinction between a physical search and an order to produce documents.[57] And second, "allow[ing] a defendant to object to the search of a third party's property."[58] Justice Alito concluded his dissent by criticizing the majority's "desire to make a statement about privacy in the digital age."[59] Whatever pragmatic value such a statement may have, the Honorable Justice Alito found it could "not justify the consequences that [the *Carpenter*] decision is likely to produce."[60]

Finally, Justice Gorsuch's dissent presents not only a property-based approach to the Fourth Amendment but also suggests how CSLI—and, by extension, other personal data—can be treated as property under the Fourth Amendment.[61] Justice Gorsuch's analysis of how personal data can be treated as property begins by noting that *Katz*'s reasonable expectation of privacy test "only 'supplements, rather than displaces the traditional property-based understanding of the Fourth Amendment.'"[62] Having established the continued functionality of property concepts under the Fourth Amendment, Justice Gorsuch elaborates on the benefits that flow from taking a property-based approach.[63]

---

52 *Carpenter*, 138 S. Ct. at 2239.

53 *Id.*

54 Freiwald & Smith, *supra* note 24, at 218.

55 *Carpenter*, 138 S. Ct. at 2247.

56 *Id.*

57 *Id.*

58 *Id.*

59 *Id.* at 2261.

60 *Id.*

61 *See Carpenter*, 138 S. Ct. at 2261–62 (introducing his analysis that sets aside *Smith* and *Miller* as ill-suited for the digital age, finding a retreat to *Katz* unnecessary, and then formulating how personal data can be treated as property under the Fourth Amendment).

62 *Id.* at 2268 (quoting Byrd v. United States, 138 S. Ct. 1518, 1526 (2018)).

63 *Id.* at 2268–71.

According to Justice Gorsuch, a property-based approach fits more readily within judicial powers than the *Katz* test because it does not ask judges to make normative judgment calls about what should be private.[64] Instead, judges are encouraged to consult the legislative branch and the common law to determine the people's rights.[65] Under a property-based approach, sharing data with a third party does not automatically eliminate an individual's rights in that data.[66] Rather, allowing a third party to hold data to process for some particular purpose is a bailment.[67] The Fourth Amendment does not require complete ownership and exclusive control for protection under a property-based approach.[68] Justice Gorsuch notes that the Fourth Amendment protects a person from an unreasonable search of her home whether or not she owns it in fee simple.[69] Moreover, an approach based on property law "may help provide detailed guidance on evolving technologies without resort to judicial intuition."[70]

In this final dissent, Justice Gorsuch openly expresses sympathy for a Fourth Amendment protection argument based on property rights under the Wireless Communications and Public Safety Act of 1999.[71] Carpenter's failure to develop this argument in the courts below led Justice Gorsuch to dismiss its viability in the case before him.[72] Perhaps intending to plant a seed for a future decision to grasp onto in recognizing property rights in personal data, Justice Gorsuch wrote: "Plainly, customers have substantial legal interests in [CSLI] including at least some right to include, exclude, and control its use. *Those interests might even rise to the level of a property right*."[73] Seizing upon this statement and the implicit treatment of personal data as property under emerging state privacy laws, a future defendant may fare well making an argument for Fourth Amendment protection on the basis that personal data is an effect.

---

64 *Id.* at 2268.

65 *Id*.

66 *Id.*

67 *Carpenter*, 138 S. Ct. at 2268 ("A bailment is the 'delivery of personal property by one person (the *bailor*) to another (the *bailee*) who holds the property for a certain purpose.'").

68 *See id*. at 2269.

69 *Id.*

70 *Id.* at 2270 ("If state legislators or state courts say that a digital record has the attributes that normally make something property, that may supply a sounder basis for judicial decision making than judicial guesswork about societal expectations.").

71 Freiwald & Smith, *supra* note 24, at 219.

72 *Id.*

73 *Carpenter*, 138 S. Ct. at 2272 (emphasis added).

III. HISTORY OF FOURTH AMENDMENT JURISPRUDENCE

The *Carpenter* Court relied upon the reasonable expectation of privacy test to protect historic cell-site location data.[74] But how does a "reasonable expectation of privacy" relate to the Fourth Amendment? And what exactly is a "reasonable expectation of privacy?" Examining the origin of the Fourth Amendment, the *Katz* decision that set this test in motion, and cases on the path from *Katz* to *Carpenter* sheds light on these questions.

A. *The Origin of the Fourth Amendment*

When the United States adopted the Fourth Amendment, American political leaders regarded *Entick v. Carrington*[75] as "'the true and ultimate expression of constitutional law' with regard to search and seizure."[76] *Entick* places striking importance on respecting property rights, stating that under English law, "the property of every man [is] so sacred, that no man can set his foot upon his neighbour's close without his leave; if he does he is a trespasser, though he does no damage at all."[77] This reverence for property presents itself in the Fourth Amendment's text. The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized.[78]

This, however, was not the text of the original draft.[79]

The Fourth Amendment's first draft used the phrase "other property" where "effects" currently stands.[80] Some debate exists as to whether this change had the impact of narrowing or expanding the scope of the Fourth Amendment,[81] but recent scholars typically agree that the impact was to narrow its scope.[82] The consensus is that the phrase "other property" indicates protection for real property, where

---

74 *Id.* at 2219.

75 95 Eng. Rep. 807 (C.P. 1765).

76 United States v. Jones, 565 U.S. 400, 405 (2012) (quoting Brower v. County of Inyo, 489 U.S. 593, 596 (1989)).

77 *Entick*, 95 Eng. Rep. at 817.

78 U.S. CONST. amend. IV.

79 Maureen E. Brady, *The Lost "Effects" of the Fourth Amendment: Giving Personal Property its Due Protection*, 125 YALE L.J. 946, 984 (2016).

80 *Id.* at 984–85.

81 United States v. Carpenter, 138 S. Ct. 2206, 2241 (2018) (Thomas, J., dissenting).

82 Brady, *supra* note 79, at 985.

"effects" excludes real property and instead extends to personal property.[83] "Effects meant, and means, 'personal property.'"[84] Recognizing personal data as personal property places it squarely within the category of "effects," facilitating an efficient route to the Fourth Amendment's protections from unreasonable searches and seizures for personal data.

But the question remains: can personal data be considered a form of personal property? The answer appears to be "yes," where personal data is rightly defined; therefore, it may qualify as an "effect." Much of the difficulty in applying the Fourth Amendment to personal data stems from the notion that data is intangible, so it cannot be considered property. In *Katz*, the focus on finding a tangible substance to protect presents itself in Justice Black's dissent.[85] While Justice Black may be correct that a conversation overheard is not tangible, his analysis failed to make the significant distinction between a conversation that is merely overheard and one that is recorded, as was the case in *Katz*.[86]

Many members of the scientific community accept the proposition that data is tangible.[87] Taking this as a fact would allow personal data to comfortably align with the Fourth Amendment's original intent to protect effects. Digitized personal information would be tangible because, under this view, "[an] asset is tangible when recorded."[88] Though the "reasonable expectation of privacy" test remains a valuable tool for affording Fourth Amendment protection where a strict property-based rationale does not apply, the Court may be able to move away from its reliance on legal fictions in this context by holding that personal data is an "effect."

---

[83] *Id.* Brady explains that "[e]ach of the ordinary dictionaries cited by the modern Court as authority for the original meaning of the Constitution defines 'effects' to mean chattels or possessions." *Id.*

[84] *Id.* at 1001.

[85] Katz v. United States, 389 U.S. 347, 365 (1967) ("A conversation overheard by . . . wiretapping, is not tangible . . . .").

[86] *Id.* at 349.

[87] *See* Ritter & Mayer, *Regulating Data as Property: A New Construct for Moving Forward*, 16 DUKE L. & TECH. REV. 220, 223 (2018) ("[T]he scientific consensus [is] that digital information is not intangible, but is physical, tangible matter."); *see also id.* at 256 ("[T]he physical quality of information, and the idea that information is a physical constituent of the universe, are widely adopted within the scientific community.").

[88] *Id.* at 257.

B. *Analyzing Katz and Its Progeny*

To understand the decision in *Carpenter*, familiarity with the origin of the "reasonable expectation of privacy" test and its application in cases that are relevant to *Carpenter*'s holding is useful. Since its inception, the reasonable expectation of privacy test has been met with criticism.[89] The foundation of these objections is the Court's departure from applying the Amendment to protect against unreasonable searches and seizures of property to broadly protecting privacy.[90] On a fundamental level, critics contend that the Court exceeded its power in creating the *Katz* test.[91] Nonetheless, the Court has continued to apply the reasonable expectation of privacy test to achieve just outcomes when faced with cases that could not have otherwise been brought under the Fourth Amendment.[92]

In *Katz*, the petitioner objected to the government's use of a recorded conversation at trial.[93] FBI agents had made the recording by placing a recording device outside of a telephone booth that Katz used to make a telephone call.[94] Katz erroneously argued that the telephone booth was a constitutionally protected area in an attempt to qualify for Fourth Amendment protection.[95] The Court rejected this argument, noting that "the Fourth Amendment protects people, not places."[96] Despite the government's arguments to the contrary, the Court held that the Fourth Amendment protects against unreasonable searches and seizures regardless of an individual's location.[97] According to the Court, a reading of the Fourth Amendment that excluded protection for

[89] *See Katz*, 389 U.S. at 364 (Black, J., dissenting) ("My basic objection is twofold: (1) I do not believe that the words of the Amendment will bear the meaning given them by today's decision, and (2) I do not believe that it is the proper role of this Court to rewrite the Amendment in order 'to bring it into harmony with the times' and thus reach a result that many people believe to be desirable.").

[90] *See id.* at 373.

[91] *Id.* (Black, J., dissenting) ("I will not distort the words of the Amendment . . . . It was never meant that this Court have such power, which in effect would make us a continuously functioning constitutional convention.").

[92] *See*, *e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018) (recognizing a reasonable expectation of privacy in the whole of one's physical movements revealed by historic CSLI); Riley v. California, 573 U.S. 373, 403 (2014) (warrant required to search cell phones given reasonable expectations of privacy in the large quantities of personal information stored on cell phones); United States v. Jones, 565 U.S. 400, 430 (2012) (stating in dicta that secretive long-term monitoring of a person's vehicle would violate reasonable expectation of privacy).

[93] *Katz*, 389 U.S. at 348.

[94] *Id.*

[95] *Id.* at 349–50.

[96] *Id.* at 351.

[97] *Id.* at 359.

conversations in telephone booths would improperly disregard the importance of the public telephone in conducting private conversations.[98]

The reasonable expectation of privacy test emerged in Justice Harlan's concurrence.[99] In its original formulation, the test had two requirements: (1) an individual actually possesses a subjective expectation of privacy in the matter at issue; and (2) that expectation is one that society would recognize as reasonable.[100] Over time, the Court has simplified the test by minimizing the first prong and looking merely at whether society would find an expectation of privacy reasonable under the circumstances of a given case.[101] In application, this is a normative test that requires judges to decide what should be private.[102] Critics vehemently oppose this result because it is impermissible for judges to substitute their judgment as to what should be protected for that of the legislature.[103]

The *Katz* decision might have come out differently if a property-based rationale had been applied. This case involved the FBI creating a digital record of an individual's conversation without his knowledge or consent.[104] This recorded conversation could be considered personal data under a broad understanding of what constitutes "personal data,"[105] but personal data definitions vary.[106] The potential outcomes under a property rationale differ starkly when taking account of these different definitions.

---

98 *Id.* at 352.

99 Carpenter v. United States, 138 S. Ct. 2206, 2236 (2018) (Thomas, J., dissenting); *see Katz*, 389 U.S. at 361.

100 *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

101 *Carpenter*, 138 S. Ct. at 2238.

102 Freiwald & Smith, *supra* note 24, at 221–22.

103 *See*, *e.g.*, *Carpenter*, 138 S. Ct. at 2236 (Thomas, J., dissenting) ("[The reasonable expectation of privacy test] invites courts to make judgments about policy, not law."); *id.* at 2265 (Gorsuch, J., dissenting) ("Deciding what privacy interests *should* be recognized . . . calls for the exercise of raw political will belonging to the legislatures, not the legal judgment proper to courts."); *see also Katz*, 389 U.S. at 374 (Black, J., dissenting) ("Certainly the Framers, well acquainted as they were with the excesses of governmental power, did not intend to grant this Court such omnipotent lawmaking authority as [to create a general right to privacy]. The history of governments proves that it is dangerous to freedom to repose such powers in courts.").

104 *Katz*, 389 U.S. at 348.

105 *See*, *e.g.*, CAL. CIVIL CODE § 1798.140(o)(1) (West 2020) (defining "personal information" as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household").

106 *See* Green, *supra* note 17.

First, there is the question of whether the recorded conversation qualifies as "personal information" at all, and then, if so, to whom it belongs. If the conversation is not viewed as personal information, then the recording would likely be viewed as the government's property, and Katz would fail to invoke Fourth Amendment protection. If it is viewed as personal information, it might belong to Katz, the person he spoke with, both of them, or—yet again—the government because the government created the recording. Katz would only be successful under a property-based approach if the recorded conversation were viewed as personal information belonging to Katz. Under this approach, Katz's recorded conversation would be his effect; accordingly, the government would need a warrant to search or seize it. Taking a property-based approach in lieu of the *Katz* test could similarly disrupt the Supreme Court's decisions in cases that followed *Katz*.

The first case following *Katz* that is relevant to *Carpenter* is *United States v. Miller*.[107] *Miller* is largely responsible for the "third-party doctrine," which postulates that a person has no reasonable expectation of privacy in data voluntarily conveyed to a third party.[108] To comply with the Bank Secrecy Act,[109] Miller's bank retained his financial transaction records.[110] The government suspected that Miller was illegally operating a distillery and failing to pay proper taxes.[111] The Alcohol, Tobacco, and Firearms Bureau accessed Miller's financial records at two banks where he was a customer with subpoenas rather than warrants.[112] The Court found that Miller's bank records were not entitled to Fourth Amendment protection because a person can maintain no reasonable expectation of privacy in records voluntarily conveyed to a third party.[113]

Like the reasonable expectation of privacy test, the third-party doctrine has received harsh criticism since its origin.[114] One source of this criticism comes from the fallacy of assuming that records are

[107] 425 U.S. 435 (1976).

[108] *Carpenter*, 138 S. Ct. at 2216.

[109] 12 U.S.C. § 1829(d) (2012).

[110] *Miller*, 425 U.S. at 436.

[111] *Id.*

[112] *Id.* at 437.

[113] *Id.* at 442–43.

[114] *See id.* at 451 (Brennan, J., dissenting) (quoting Burrows v. Superior Court, 13 Cal. 3d 238 (1974)) ("To permit a police officer access to these records merely upon his request, without any judicial control . . . opens the door to a vast and unlimited range of very real abuses of police power."); *see also id.* at 456 (Marshall, J., dissenting) (proposing that retaining records pursuant to the Bank Secrecy Act is itself an unconstitutional seizure; therefore, law enforcement cannot constitutionally access these records).

voluntarily conveyed.[115] Reliance on property rights may have avoided these difficulties because the information conveyed to a third party for a limited purpose could be considered a bailment—a transfer of possession for a certain limited purpose without surrendering ownership rights.[116]

Under a property-based theory, *Miller* may or may not have come out differently. The Court could have found that the seizure of Miller's financial records violated the Fourth Amendment because Miller held property rights in those records although the bank possessed them for certain limited purposes. Alternatively, the Court may have found that the government's access to Miller's financial records was lawful because the search or seizure was reasonable. Keep in mind that the Fourth Amendment only prohibits those searches and seizures of persons, houses, papers, or effects that rise to the level of unreasonable.[117] It is feasible that the Court would have concluded that Congress, in enacting the Bank Secrecy Act, properly recognized that a search or seizure is reasonable under these circumstances. On the other hand, employing a property-based rationale could have led to Miller's records being the bank's property. Miller would not be able to assert a Fourth Amendment right to his bank records if they were deemed the bank's property.

Smith v. Maryland[118] is the next case relevant to *Carpenter*. This case is analogous to *Miller*, as it also involves warrantless access to information conveyed to a third party.[119] In *Smith*, the Court held that Smith had voluntarily assumed the risk that the phone company would convey the phone numbers he dialed to law enforcement.[120] Because Smith had assumed that risk, the Court found that he had no reasonable expectation of privacy in the records of phone numbers that he had dialed.[121]

---

115 *Id.* at 451(Brennan, J., dissenting) (quoting Burrows v. Superior Court, 13 Cal. 3d 238 (1974)) ("For all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account."); *see also* Smith v. Maryland, 442 U.S. 735, 746–47 (1979) (quoting Katz v. United States, 387 U.S. 347, 352 (1967)) (Stewart, J., dissenting) (noting that records of phone numbers that an individual dials are not truly voluntarily conveyed given the "vital role that the public telephone has come to play in private communication[s]").

116 *See* Carpenter v. United States, 138 S. Ct. 2206, 2268 (2018) (Gorsuch, J., dissenting).

117 U.S. CONST. amend IV.

118 442 U.S. 735, 736 (1979).

119 *See id.* at 745–46.

120 *Id.* at 744.

121 *Id.* at 745.

Justice Stewart dissented on the ground that people do have a reasonable expectation of privacy in the numbers that they dial.[122] Justice Marshall also dissented, powerfully articulating the dangers of unregulated government monitoring: "Permitting governmental access to telephone records on less than probable cause may thus impede certain forms of political affiliation and journalistic endeavor that are the hallmark of a truly free society."[123] To the majority, however, the third-party doctrine dictated the result—the government would not be required to obtain a warrant before accessing an individual's records at the telephone company.[124]

Smith attempted to argue that the Court should find his expectation of privacy reasonable because he had made calls without a live operator.[125] These calls were processed through switching equipment that could only "remember" numbers if programmed to do so.[126] The Court rejected this argument, noting the "crazy quilt" of a rule that would result if petitioner's suggestion were adopted.[127] The Court's desire to avoid "mak[ing] a crazy quilt of the Fourth Amendment"[128] is admirable, but continuing to apply the reasonable expectation of privacy test with the third-party doctrine at times appears to do just that.

Congress responded to the issues in *Smith* with legislation. The Pen Register Statute,[129] requires the government to obtain a court order prior to installing a pen register.[130] While this allows the use of pen registers without requiring a warrant, the government must demonstrate that "the information likely to be obtained is relevant to an ongoing criminal investigation."[131] This Congressional enactment reflects the fact pen register data falls outside of the current understanding of the Fourth Amendment's scope.

122 *Id.* at 747.

123 *Id.* at 751.

124 *Smith*, 442 U.S. at 743–44.

125 *Id.* at 745.

126 *Id.*

127 *Id.* at 745 ("We are not inclined to make a crazy quilt of the Fourth Amendment, especially in circumstances where (as here) the pattern of protection would be dictated by billing practices of a private corporation.").

128 *Id.*

129 18 U.S.C. §§ 3121–3127 (2012).

130 BALDWIN'S OHIO PRACTICE CRIMINAL LAW § 4:20 RIGHT OF PRIVACY—PEN REGISTERS (2019).

131 18 U.S.C. § 3122(b)(2).

Next, the case of *United States v. Jones*[132] warrants discussion. *Jones* is more analogous to the facts at issue in *Carpenter*, as it is the first case where the Court begins to address law enforcement's use of modern surveillance technology.[133] In *Jones*, the government installed a global positioning system (GPS) device on Jones's wife's car after its warrant to do so expired.[134] In addition, the warrant only authorized government action in the District of Columbia, but the government attached the GPS device when the car was in Maryland.[135] Ultimately, the Court decided this case based on physical trespass into the vehicle, but "five justices agreed that a surreptitious long-term monitoring of the vehicle also impinged on reasonable expectations of privacy, even if those movements were in public view."[136] Justice Scalia wrote for the majority: "[i]t is beyond dispute that a vehicle is an 'effect' as that term is used in the [Fourth] Amendment."[137]

The *Jones* Court's reliance on the right to be free from physical trespass (despite recognizing a reasonable expectation of privacy in dicta) reveals a preference for a property-based rationale over *Katz*'s legal fiction. If the two stood on equal ground, the Court could have held the Fourth Amendment was violated on both grounds, but it did not. The *Jones* Court avoided the problematic reasonable expectation of privacy test entirely in its holding and merely paid homage to *Katz*'s precedent in dicta.[138]

Justice Sotomayor wrote a powerful concurrence that cautions against permitting an overly permeating police surveillance.[139] "Awareness that the government may be watching chills associational and expressive freedoms. . . . GPS monitoring . . . may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'"[140] Justice Sotomayor went on to question whether the third-party doctrine should be reconsidered, as it is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane

132 565 U.S. 400 (2012).

133 Freiwald & Smith, *supra* note 24, at 216.

134 *Jones*, 565 U.S. at 402–03.

135 *Id.* at 403.

136 Freiwald & Smith, *supra* note 24, at 216–17.

137 *Jones*, 565 U.S. at 404.

138 Freiwald & Smith, *supra* note 24, at 222 n.152 ("The *Jones* Court recognized that nontrespassory acquisitions of location data would involve a *Katz* analysis, but it put off conducting that analysis and the 'thorny problems' associated with it for another day.").

139 *See Jones*, 565 U.S. at 413–18 (Sotomayor, J., concurring).

140 *Id.* at 416 (Sotomayor, J., concurring) (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

tasks."[141] Indeed, recognizing that personal data is personal property—as an effect subject to Fourth Amendment protection—could alleviate these concerns. There would be no need to invoke the third-party doctrine and the *Katz* test under a property-based rationale taking this approach to personal data.

A final case worth considering on the path from *Katz* to *Carpenter* is *Riley v. California*.[142] Riley objected to law enforcement's search of the data on his cell phone after he was arrested.[143] Generally, the law recognizes a broad exception to the Fourth Amendment for a search incident to an arrest.[144] The Court's holding narrowed this exception to exclude searching the data stored on cell phones.[145] Cell phones have a unique tendency to store vast amounts of personal information. This served as the foundation for the Court's decision to exempt cell phone data from the traditional Fourth Amendment exception for searches incident to an arrest.[146] The Court recognized the widespread use of cell phones in American society and the pervasive nature of the personal information that these devices typically store.[147]

California attempted to argue for a limited warrant requirement for cell phone searches on a variety of grounds.[148] Ultimately, the Court decided to impose a general categorical restriction on searches of cell phone data incident to arrest.[149] The Court emphasized the need to provide clear guidance to law enforcement in order to avoid "a difficult line-drawing expedition."[150]

---

141 *Jones*, 565 U.S. at 417.

142 573 U.S. 373 (2014).

143 *See id.* at 378–79.

144 Aldrich, *supra* note 22, at 5.

145 *Id.*

146 Freiwald & Smith, *supra* note 24, at 217; *Riley*, 573 U.S. at 386 ("Cell phones . . . place vast quantities of personal information literally in the hands of individuals. . . . [O]fficers must generally secure a warrant before conducting [a search of data on a cell phone].").

147 *Riley*, 573 U.S. at 395 ("[M]any of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate.").

148 *Id.* at 398–400 (allowing searches of arrestee's cell phones if officers limited to "areas of the phone where an officer reasonably believes that information relevant to the crime, the arrestee's identity, or officer safety will be discovered," the call log, and "if [officers] could have obtained the same information from a pre-digital counterpart.").

149 *Id.* at 398 (quoting Michigan v. Summers, 452 U.S. 692, 705 n.19 (1981)) ("[I]f police are to have workable rules, the balancing of the competing interests . . . 'must in large part be done on a categorical basis—not in an ad hoc, case-by-case fashion by individual police officers.'").

150 *Id.* at 401.

Recognizing that personal data is personal property would be consistent with the Court's desire to provide a clear categorical rule. The failure to do so has left lower courts reluctant to require a warrant under the Fourth Amendment in cases involving search and seizure of personal data after *Carpenter*.[151] In an effort to be prudent, courts are interpreting *Carpenter* narrowly.[152] While not requiring a warrant to search and seize personal data may avoid an impediment in law enforcement's ease of access to such data, it is likely causing more harm than good by subjecting citizens to unreasonable search and seizure of their personal data. Accepting personal data as an effect could provide clear notice to law enforcement that a warrant is required to search or seize these sensitive digital records—helping to secure individuals' right to be free from unreasonable search and seizure in the digital era.

IV. PERSONAL DATA IS TREATED AS PROPERTY UNDER STATE DATA PRIVACY LAWS

"[T]he divergence between the law in books and law in action is more acute in some periods of legal history than in others."[153] Scholars argue that "data has now become a new kind of property—an asset that is created, manufactured, processed, stored, transferred, licensed, sold, and stolen."[154] In today's rapidly advancing technological era, courts and legislatures grapple with protecting personal data.[155] Under the guise of increasingly expansive privacy laws, state legislatures are imparting property rights in personal data.

It is not within the province of the Court to decide what property rights should be. State legislatures and the common law are typically responsible for both creating and safeguarding individuals' property rights.[156] But what has yet gone unnoticed is the fact that the states are

---

151 *See* Grande, *supra* note 13 ("[d]istrict courts have been reluctant to require warrants for access to digital records beyond the historical cellphone location data covered by the U.S. Supreme Court's [*Carpenter*] decision."); *see also* Aldrich, *supra* note 22, at 7 (discussing *United States v. Oakes*, No. 3:16-cr-00196 (M.D. Tenn. July 31, 2018), where the court denied Fourth Amendment protection to access of a defendant's location through search and seizure of CSLI under the premise that *Carpenter* only applied to CSLI related to one's phone).

152 *See* Grande, *supra* note 13; *see also* Aldrich, *supra* note 22, at 6–7.

153 Pound, *supra* note 1, at 22.

154 Ritter & Mayer, *supra* note 87, at 221.

155 *See, e.g.*, United States v. Carpenter, 138 S. Ct. 2206 (2018) (historic cell-site location information); *see also Riley*, 573 U.S. 373 (data stored on a smartphone); Illinois Biometric Information Privacy Act of 2008, 740 ILL. COMP. STAT. 14 (2008); CAL. CIV. CODE §§ 1798.100–1798.199 (West 2020).

156 *See*, *e.g.*, Katz v. United States, 389 U.S. 347, 350–51 (1967) (stating that protection of persons' property is mainly the responsibility of state legislatures); *see also* Pamela

beginning to grant property rights in personal data while continuing to apply the label of "privacy." State legislatures employ a legal fiction by speaking of personal data as if it were only protected by privacy rights—but their actions continually extend property rights to personal data. The Court could take notice of this reality and recognize that personal data is a form of property protected under the Fourth Amendment. Waiting for the legislatures to make the leap to reclassify personal data as property may be a mistake, as the risks that come with changes in law stymie change even in the face of pressing reasons to alter the law.[157]

A. *Privacy vs. Property: What's the Difference?*

While privacy says "you cannot see" or "you cannot know," property says "you cannot possess, use, or modify."[158] Louis D. Brandeis and Samuel D. Warren's *The Right to Privacy*[159] is the seminal work on privacy scholarship.[160] In their article, Brandeis and Warren describe a privacy right as "the right to one's personality."[161] Privacy allows individuals to maintain their unique, authentic selves by providing a shield from unwanted criticism. The scholars explain that the right to privacy applies to "personal writings and any other productions of the intellect or of the emotions."[162] They argue that "privacy for thoughts, emotions, and sensations . . . should receive the same protection, whether expressed in writing, or in conduct, in conversation, in attitudes, or in a facial expression."[163] According to these scholars'

Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1142 (2000) ("Grants of property rights are generally the province of state law."). S*ee generally* Carol M. Rose, *Possession as the Origin of Property*, 52 U. CHI. L. REV. 73, 77 (1985) (discussing various theories of property that emerged from the common law).

157 *See* Pound, *supra* note 1, at 14; *see also* Freiwald & Smith, *supra* note 24, at 223 (arguing that deference to the legislature is a flawed approach because Congress "recognized the cell phone tracking problem but was content to legislate on the margins, deferring to courts on the hard question of legal standards").

158 *Compare* Daniel E. Newman, *European Union and United States Personal Information Privacy, and Human Rights Philosophy—Is There a Match?*, 22 TEMP. INT'L & COMP. L.J. 307, 311–14 (2008) (noting the prevailing philosophical justifications for privacy being to "avoid unwilling exposure of personal information" and protect "the desire for freedom from observation"), *with* Brady, *supra* note 79, at 994 ("Personal property gives its owner a right to exclude others from possessing, using, and interfering with the effect.").

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

160 *See* Newman, *supra* note 158, at 310.

161 Brandeis & Warren, *supra* note 159, at 207.

162 *Id.* at 213.

163 *Id.* at 206.

thesis, objects of privacy are incorporeal, though they may be embodied in various media. In general, a privacy right functions to exclude others from nonconsensual access to the object of the privacy interest.[164]

There are a number of philosophical justifications for privacy.[165] Three of the major philosophical justifications for privacy apply specifically to personal information privacy.[166] The first deals with "socialization and freedom from unwilling exposure."[167] Under this theory, privacy functions to preserve the personality.[168] By placing limits on others' access to oneself, an individual can avoid social pressure to change.[169] Additionally, privacy plays an important role in socialization by facilitating intimate relationships.[170] Privacy allows an individual to create a realm of secret information known only to those specially selected to share in intimacy.

The second relevant philosophical justification for privacy in one's personal information is "interiority and freedom from observation."[171] This theory provides that privacy benefits individuals by allowing for secrecy, anonymity, and solitude.[172] "Interiority" allows an individual to exercise critical thought free from social pressure, and it is the pre-requisite for self-reflection.[173] This gives individuals the ability to develop challenges to popular ideas, formulate unique perspectives, and develop a strong sense of self.

The third philosophical justification for privacy in personal information relates, not to an individual's benefit, but to the benefit of society.[174] Through privacy, individuals gain the freedom that allows for the development and contribution of unique perspectives to public debate.[175] From this perspective, the ultimate beneficiary of privacy rights is not the individual but society as a whole. In all three theories, there is a volitional aspect to the object of the privacy right. Privacy is protecting the product of one's thoughts and emotions from scrutiny

164 *See* Newman, *supra* note 158, at 311 (noting that "the concept of consent is a common thread, of varying degrees of import, underlying all three [main philosophical justifications for privacy]").

165 *See id.* at 310–11.

166 *Id.*

167 *Id.* at 311.

168 Newman, *supra* note 158, at 311.

169 *Id.*

170 *See id.* at 312.

171 *Id.* at 314.

172 *See id.*

173 *Id.* at 315.

174 Newman, *supra* note 158, at 317.

175 *Id.*

and pressure to change. If violated, the objects of privacy may cease to exist, as one may abandon unpopular ideas, avoid expression of quirky personality traits, or neglect to pursue curious endeavors.

Moving from an analysis of privacy to an analysis of property, keep in mind the volitional nature of the objects of privacy rights, and note the contrast in the nature of the objects of property rights. Broadly speaking, the concept of property encompasses all that an individual possesses.[176] From this standpoint, an individual's real property, chattel, intangible products of the mind, privileges, and rights—including the right to privacy—are all objects of property.[177] If the objects being protected have a volitional nature, the shift from the broad category of property into the subset of privacy is justified. The protections given by a privacy right protect this volitional nature by preventing unwanted exposure and freedom from observation.

Property rights generally apply to static objects, both tangible and intangible, with an exception for the subset of objects of privacy.[178] Under the Fourth Amendment, the question is whether personal data is properly protected by privacy rights (and, therefore, can only be brought under the Fourth Amendment through the use of the *Katz* test), or whether personal data properly belongs among the more general objects of property rights entitled to direct, categorical protection from unreasonable search and seizure.

A "property right" is essentially "the right to exclude."[179] Pragmatically, there is a difference between the function of property rights and privacy rights. Privacy functions to avoid unwanted exposure or observation.[180] Property functions to prevent unwanted possession, use, and interference with its objects.[181] Examining emerging trends in data privacy law reveals the fact that personal data is not merely being shielded from exposure or observation; rather, it is being protected from unwanted possession, use, and interference. While state legislatures have not gone so far as to declare a property right in personal data, likely due to the practical difficulties that may arise with

176 *See* Brandeis & Warren, *supra* note 159, at 193.

177 *Id.*

178 *See id.* (stating that the original objects of a property interest were "lands" and "cattle" but noting that the concept property has grown to encompass intangible objects as well).

179 Mark A. Lemley & Philip J. Weiser, *Should Property or Liability Rules Govern Information?*, 85 TEX. L. REV. 783, 783 (2007).

180 Newman, *supra* note 158, at 311–14.

181 Brady, *supra* note 79, at 994.

doing so,[182] the Court need not overlook what is actually happening. Personal data is being treated as property under state data privacy laws.

Perhaps the reason that state legislatures have not classified personal data as property stems from the difficulty of reconciling personal data with preexisting notions of property. The doctrine of first possession awards property rights to one who first provides "notice to the world through a clear act."[183] Inherent in this theory is a reward for useful labor.[184] Take, for example, the classic case of *Pierson v. Post*.[185] In *Pierson*, the court awarded property rights to an interloper who shot a fox as it was being pursued by another hunter.[186] The majority found that the property right belonged to the individual who executed a clear act evidencing "an unequivocal intention of appropriating the animal to his individual use."[187] The court rewarded the labor that went into hunting the fox by holding that the act created a property right.

Scholars argue that personal data should belong to the person to whom it relates.[188] Indeed, this is the effect given by state data privacy laws.[189] But the person whom personal data relates to often exercises little or no labor in creating the data. Biometric identifiers are immutable physical traits that individuals carry throughout life (retinal patterns, fingerprints, face geometry, etc.). Some personal identifiers are assigned to individuals at birth (first name, last name, and social security number). Other forms of personal data are created through copious amounts of labor on the part of companies recording the data, and only incidentally by the actions of individuals to whom the data relates (internet browsing history, search history, CSLI, etc.).

Granting property status to personal data is at odds with the labor-based notion of property. Nonetheless, legislatures are beginning to treat personal data as if it were property that belonged to the individual to whom it relates. The Court may take notice of this fact and hold that personal data is also property under the Fourth Amendment. The following Section explores the ways that state data privacy laws treat personal data as property.

---

182 *Infra* Part VI.

183 Rose, *supra* note 156, at 77.

184 *Id.*

185 3 Cai. R. 175 (1805).

186 *Id.* at 178.

187 *Id.*

188 Ritter & Mayer, *supra* note 87, at 229–30; *see also* Elvy, *supra* note 17, at 463 n.210.

189 *See infra* Section IV.B.

B. *Property Protections for Personal Data Under State Data Privacy Laws*

1. Illinois Biometric Information Privacy Act of 2002

As technology advances, the amount and nature of personal data available continue to increase. The Illinois Biometric Information Privacy Act of 2008[190] (BIPA) was the first state legislation to grant heightened protection to a new class of highly sensitive personal data—biometric identifiers. Today six states (Illinois, Texas, New York, Arkansas, California, and Washington) have a law protecting biometric information.[191] BIPA is significant because it treats biometric identifiers like property by providing for a cause of action on a statutory violation alone; there is no need to establish a separate injury for the law to recognize that rights have been violated.[192] Recall that *Entick*,[193] the reputed ultimate expression of the law on search and seizure at the time drafters wrote the Fourth Amendment,[194] provides that "the property of every man [is] so sacred, that no man can set his foot upon his neighbour's close without his leave; if he does he is a trespasser, though he does no damage at all."[195] This special protection afforded to property differs from the general requirement for a concrete injury in fact.[196] BIPA stands as the first prominent example of affording an implicit property right in personal data.

190 Illinois Biometric Information Privacy Act of 2008, 740 ILL. COMP. STAT. 14 (2008).

191 The Anatomy of Biometric Laws: What Companies Need to Know in 2020, THE NAT'L L. REV. (Jan. 15, 2020), https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020.

192 Rosengrant v. Six Flags, 129 N.E.3d 1197, 1207 (Ill. 2019) ("[A]n individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an 'aggrieved' person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act.").

193 Entick v. Carrington, 95 Eng. Rep. 807 (C.P. 1765).

194 United States v. Jones, 565 U.S. 400, 405 (2012) (quoting Brower v. County of Inyo, 489 U.S. 593, 596 (1989)).

195 *Entick*, 95 Eng. Rep. at 817.

196 *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016) (finding the plaintiff failed to allege a concrete injury under the Fair Credit Reporting Act, 15 U.S.C. § 1681, when the defendant published inaccurate data about him in its credit reporting service).

2. The California Consumer Privacy Act of 2018

Traditionally, the U.S. approach to data privacy has focused on regulating the actions of entities that collect data rather than providing individuals with control over the use of their data.[197] The California Consumer Privacy Act of 2018[198] (CCPA) disrupted this trend, and a number of states are ramping up to follow suit.[199] The CCPA set a revolutionary precedent for United States privacy laws. California has a history of influencing other state legislatures to enact progressive laws as citizens' needs change in response to modern innovations.[200] Other states have already begun drafting comprehensive personal data privacy laws modeled after the CCPA.[201]

The European Union's General Data Protection Regulation (GDPR) influenced the CCPA's protections.[202] Both the GDPR and the CCPA provide personal data with protections traditionally afforded to property, rather than the simple protections from unwanted access or observation germane to privacy rights. The GDPR provides citizens of the European Union with protection from "unwanted possession"—"the right to be forgotten"[203] by deletion of personal data on request; "unwanted use"—"the right to object"[204] to unwanted data processing; and "unwanted interference"—"the right to rectification"[205] if personal data is inaccurate or incomplete.[206] The CCPA extends two of these three traditional property rights to personal data: "unwanted possession" through the right to deletion;[207] and "unwanted use" by the right to object[208] to third-party data processing.[209] These provisions

197 Newman, *supra* note 158, at 319.

198 CAL. CIVIL CODE §§ 1798.100–1798.199 (West 2020).

199 *See* Catherine Barrett, *Are the EU GDPR and the California CCPA Becoming the De Facto Global Standards for Data Privacy and Protection?*, 15 SCITECH LAWYER 24, 27 (Spring 2019) (observing that the CCPA elevates protection in personal data privacy to a fundamental right); *see also* Green, *supra* note 17.

200 *See* Barrett, *supra* note 199, at 27 ("California laws often serve as a model for other state legislatures.").

201 *See* Green, *supra* note 17.

202 Sarah Hospelhorn, *California Consumer Privacy Act (CCPA) vs. GDPR*, VARONIS (June 17, 2020), https://www.varonis.com/blog/ccpa-vs-gdpr.

203 Directive 2016/679, 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 and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) 2016 O.J. (119) 1,13. [hereinafter "GDPR"].

204 *Id.* art. 21.

205 *Id.* art. 16.

206 Barrett, *supra* note 199, at 27.

207 CAL. CIVIL CODE § 1798.105 (West 2020).

208 *Id.* § 1798.120.

209 Barrett, *supra* note 199, at 27.

vest individuals not with privacy rights but with *ownership* rights in their personal data.[210]

3. Comprehensive State Personal Data Privacy Legislation Outside of California

Like the CCPA, other states are moving to enact data privacy laws that give individuals increased control over their personal data.[211] The right to delete is included in pending bills in New York, Maryland, Massachusetts, and Hawaii.[212] This right goes to the core concept of property—excluding others from unwanted possession.[213] Contrast this with privacy's protection from unwanted access to prevent undesired criticism, humiliation, or pressure to change. These state laws do not merely require businesses to cease processing personal data, which would be sufficient to protect privacy rights; they require deletion—completely relinquishing possession.

Some states' proposed bills go even further than the CCPA in terms of granting their citizens implicit property rights in personal data. Similar to BIPA, Massachusetts's proposed bill includes a private right of action for any violation of the law, irrespective of whether an individual suffered any actual "loss of money or property as a result of the violation."[214] In New York's proposed bill, any violation at all constitutes grounds for a private right of action.[215] New York also vests citizens with a right to correct information held about them.[216] This is a "right to rectification"—the property protection allowing individuals to be free from unwanted interference that is found in the GDPR.[217] Additionally, New York creates a "data fiduciary" role imposing upon businesses a duty to "exercise the duty of care, loyalty and confidentiality expected of a fiduciary with respect to securing the personal data of a consumer against a privacy risk; and . . . act in the best interests of the consumer, without regard to the interests of the entity, controller or data broker."[218] New York's proposed law goes on to provide a broad right to opt-out of personal data processing, in contrast to the right to opt-out of personal information sales found in the

210 Hospelhorn, *supra* note 202.
211 *See* Green, *supra* note 17.
212 *Id.*
213 Lemley & Weiser, *supra* note 179.
214 Green, *supra* note 17.
215 *Id.*
216 *Id.*
217 GDPR, *supra* note 203, art. 16.
218 Green, *supra* note 17.

CCPA.[219] Maryland's law surpasses the CCPA's protections by requiring disclosure of all personal data shared with third parties, even if provided for free.[220]

Presently, state laws governing the treatment of personal data are undergoing a metamorphosis. Our nation is at a point where an implicit treatment of personal data as property is emerging. The origin of this change is visible in BIPA, where an individual can sustain a cause of action without showing injury in fact. The CCPA and copycat statutes on the horizon take the property-like treatment of personal data to the next level by granting protections against unwanted possession, use, and interference. The Court could use these state laws as a basis for recognizing personal data as personal property—an "effect"—under the Fourth Amendment. This could allow for smooth and consistent protection for personal data from warrantless search and seizure.

C. *State Data Privacy Laws Apply to Objects Suited for Property Rights*

To decide whether property rights or privacy rights are best suited to protect a given object, a relevant consideration is whether the object of the right is the product of one's volition, such that one would benefit from preventing unwilling exposure or observation.[221] As explained above, state data privacy laws purport to provide privacy rights, but in effect, afford protections given to property.[222] The case for finding that personal data is property is strengthened by recognizing that the objects of these data privacy laws are better classified as property.

BIPA covers "biometric identifiers."[223] The definition of "biometric identifiers" includes "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[224] "Biometric information" includes "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual."[225] Each of these items is static, hence the usefulness of biometric identifiers in identifying an individual. The concerns for protecting these objects do not stem from a desire to avoid exposure or observation for fear of humiliation or undue social pressure to change;

---

219 *U.S. State Comprehensive Privacy Law Comparison*, INT'L ASS'N OF PRIVACY PROFESSIONALS: PRIVACY TRACKER (Apr. 18, 2019), https://iapp.org/news/a/us-state-comprehensive-privacy-law-comparison/.

220 Green, *supra* note 17.

221 *See supra* Section IV.A.

222 *See supra* Section IV.B.

223 Illinois Biometric Information Privacy Act of 2008, 740 ILL. COMP. STAT. 14 (2008).

224 *Id.* § 10.

225 *Id.*

rather, the concerns for protecting this information stem from the desire to control possession, use, and interference with this highly sensitive personal data.[226] If a nefarious party were to possess another individual's biometric identifiers wrongfully, that individual could be subjected to tampering with financial records, security screenings, and identity theft.[227] BIPA is one example illustrating the fact that classifying personal data as an object of privacy rather than property is a legal fiction.

The CCPA also includes objects more readily described as objects of property rights than of privacy rights. Under the CCPA, "personal information" is "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[228] The statute includes a list of examples, including a real name, postal address, records of personal property, biometric information, internet browsing history, search history, and geolocation data.[229] The protections extend beyond objects sure to identify an individual to "probabilistic identifiers" defined as "the identification of a consumer or a device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information."[230] The CCPA excludes publicly available information.[231]

The CCPA includes an expansive definition of personal information. Many of the CCPA's objects have little or nothing to do with an individual's thoughts or emotions—biometric identifiers, postal address, real name, and records of personal property. The stated purpose and intent of the CCPA is to "further Californians' right to privacy by giving consumers an effective way to control their personal information."[232] But individuals are being given control over these objects for the purpose of controlling their use and possession.[233] Granted, some of the objects that fall under the CCPA's expansive definition of privacy may rightly be thought of as objects best suited for privacy protections (internet search and browsing histories, for

226 *Id.* § 5(g) ("The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.").

227 *Id.* § 5.

228 CAL. CIVIL CODE § 1798.140(o)(1) (West 2020).

229 *Id.* § 1798.140(o)(1).

230 *Id.* § 1798.140(p).

231 *Id.* § 1798.140(o)(2).

232 2017 Cal. AB 375 § 2(i) (June 28, 2018).

233 *See supra* Section IV.B.

example). The fact that there are mixed objects and mixed motives under the CCPA does not detract from the fact that an implicit grant of property status is given to personal information. The protections afforded to all objects of the CCPA are those generally afforded to property.

Tellingly, even the CCPA's exclusion of publicly available information is consistent with an understanding that personal information is treated as property for Fourth Amendment purposes. In *Oliver v. United States*,[234] the Court held that the Fourth Amendment does not protect "open fields" from warrantless searches by law enforcement.[235] Publicly available information is analogous to an open field in that an individual does not share the same intimate connection with publicly available information as with information known only by oneself and an intentionally selected group of others. Further, open fields are not "effects," as an "effect" is an item of personal, not real property.[236] Excluding publicly available information from classification as an effect is consistent with this premise.

Legislatures have been cautious in extending property rights to personal data. They are doing so by developing the legal fiction that stretches privacy rights to afford protections never before given by privacy law to objects never before subject to privacy law. While these laws will serve to give individuals heightened protection, more is needed to ensure individuals' personal data is secured from abuse. The states may be best advised to continue using the legal fiction of expanding the concept of privacy, as explained in Part VI below; however, the Court could recognize personal data as property to afford Fourth Amendment protection to personal information in order to allow for the efficient administration of justice, to provide clear notice to law enforcement as to warrant requirements and ensure individuals' freedom from unreasonable searches and seizures.

V. PROMOTING EFFICIENCY IN APPLYING THE FOURTH AMENDMENT

"The face of the law may be saved by an elaborate ritual, but men, and not rules, will administer justice."[237] The Court stretched the text of the Fourth Amendment to create the reasonable expectation of privacy test to administer justice when it had no other way to do so. While this device may remain useful, perhaps even necessary in certain contexts, the time has arrived when the reasonable expectation of privacy test

234 466 U.S. 170 (1984).
235 *Id.* at 178–84.
236 Brady, *supra* note 79, at 1001.
237 Pound, *supra* note 1, at 20.

may no longer be needed to protect personal data from unreasonable searches and seizures. Recognizing property rights in personal data would allow the Fourth Amendment to directly protect personal data from unreasonable search and seizure as an "effect."

Pound noted the problem with legal fictions long ago: "until the law has evolved some device by which [individuals] may use it in all cases the weak and friendless and lowly will be at a practical disadvantage, despite the legal theory."[238] As Pound observed, changes in law present risks.[239] This fact results in legislatures hesitating before implementing needed changes in the law.[240] Further, political tensions can hinder the legislative process, making it difficult for controversial new laws to pass. It may not be for many years, if ever, that the legislature outright declares personal data as property. This leaves the most vulnerable members of society at the greatest risk of failing to receive protection for their personal data under the Fourth Amendment.

Fortunately for individuals, the United States Supreme Court is now primed to grant protection to personal data by recognizing personal data as property belonging to the individual that it relates to. "Fourth Amendment law is constructed by the 'concepts' and 'understandings' that derive from social life and myriad state laws . . . ."[241] Following along this natural course, the Court may first recognize that a property right in personal data exists implicitly under state legislation, and then hold that the Fourth Amendment applies to personal data as an effect.

It seems that the Court has been awaiting a moment to decide whether or not property rights exist in data for some time now. Justice Scalia stated that whether or not computer data is an "effect" is "a really good question."[242] Justice Scalia refrained from answering a student from Brooklyn Law School who asked whether computer data is an effect, noting that "[t]hat's something that may well come up."[243] Justice Gorsuch discussed the viability of an appeal to positive law in *Carpenter* for protecting CSLI under the Fourth Amendment but noted that Carpenter had waived that right by failing to assert it in courts below.[244]

---

238 *Id.* at 17.

239 *Id.* at 12.

240 *See id.* at 14.

241 Brady, *supra* note 79, at 1002.

242 Debra Cassens Weiss, *Does the Fourth Amendment Protect Computer Data? Scalia Says It's a Really Good Question*, ABA JOURNAL (Mar. 24, 2014, 1:06 PM), http://www.abajournal.com/news/article/asked_about_nsa_stuff_scalia_says_conversations_arent_protected_by_fourth_a.

243 *Id.*

244 Freiwald & Smith, *supra* note 24, at 219.

The time may have arrived where, given the right case or controversy, the Court will hold that personal data is a form of property.

A. *Defining Personal Data*

Personal data will need to be precisely defined to comport with due process requirements for fair notice and to avoid arbitrary enforcement of the law. Advancements in technology demand adjustments in law to maintain the proper balance between liberty and security.[245] Lower courts need guidance from the Supreme Court to handle challenges presented by modern technology, and law enforcement needs guidance to prevent overly permeating police surveillance.[246] *Carpenter* dealt with historic CSLI, but this is not the only form of personal data that ought to be brought under the Fourth Amendment. In crafting a definition for personal data under the Fourth Amendment, the Court should look to state data privacy laws for guidance,[247] ensure that new forms of sensitive data that are likely to develop will be covered, and provide an intelligible definition that benefits both courts and citizens.

Under this analysis, the most appropriate definition for personal data may be limited to those objects that exist independently of a person's volition. Biometric identifiers and biometric information should certainly fall under this definition, for not only do they exist independent of an individual's will, but they are also largely unchangeable. Other candidates to include are items that bear little relation to intimate thoughts or emotions. For example, a person's real name, street address, IP address, date of birth, and social security number are best understood as objects of property since the risk of abuse lies not in unwanted exposure or observation but in unwanted possession, use, or interference.

Alternatively, a broadly defined concept of personal information could alleviate the struggle found in more Fourth Amendment cases that invoke *Katz*'s reasonable expectation of privacy test. Katz's conversation, for example, could be considered personal information under the CCPA once recorded because it is capable of identifying Katz.[248] The third-party doctrine may also decrease in utility if the definition of personal data were to follow the path of the CCPA by

245 *See generally* Freiwald & Smith, *supra* note 24 (describing the interplay that new technologies create by providing new tools for both criminals and law enforcement agents).

246 *See id.* at 206.

247 Brady, *supra* note 79, at 1002 ("Fourth Amendment law is constructed by the 'concepts' and 'understandings' that derive from social life and myriad state laws.").

248 *See* CAL. CIVIL CODE § 1798.140(o)(1) (West 2020).

excluding publicly available information from the definition of personal data.[249] One difficulty with taking up the broadly expansive definition of personal data used under the CCPA is that it fails to provide clear notice as to what exactly personal data is. The notion of "probabilistic identifiers" is particularly vague, employing a standard of being "more probable than not" that information identifies a consumer or device.[250] If the goal is a categorical rule providing clear notice to individuals and law enforcement, a narrower definition of personal data may be best.

VI. IMPLICATIONS OF DECLARING PROPERTY RIGHTS IN PERSONAL DATA

Holding that personal data is an effect under the Fourth Amendment would have substantial implications. While individuals would presumably enjoy constitutional protection over their data, the pervasive and varied nature of data can create confusion, rather than provide clarity, when applying a warrant requirement. This Part explores challenges that may arise if personal data were recognized as an effect.

A. *Implications of Treating Data as Property Under the Fourth Amendment*

Recognizing personal data as property is likely to be met with its fair share of backlash. The government may argue an impediment in prosecuting criminals, scholars may object on philosophical grounds, and businesses may fight vehemently on the grounds of an undue burden.[251] Such a reaction should come as no surprise—it is known that changes in the law are dangerous.[252] The likelihood of this backlash ought not to prevent the Court from recognizing that personal data is property for two reasons: (1) personal data is rightly understood as an effect, and (2) all of these criticisms can be quieted.

First, consider those who argue that declaring a property right in personal data would impede law enforcement in prosecuting criminals. Law enforcement is not left without access to personal data under this approach. Rather, law enforcement officers must simply comply with the Fourth Amendment requirement to ensure a search is reasonable. By demonstrating probable cause and acquiring a warrant, law enforcement can search and seize personal data.

---

249 *Id.* § 1798.140(o)(2).

250 *Id.* § 1798.140(p).

251 This objection is discussed in Section VI.B.

252 Pound, *supra* note 1, at 12.

Next, consider the philosophical objections that scholars are bound to launch. As discussed in Part III above, the mistaken belief that data is intangible will likely be hurled critically at the Court. But this conception lacks the scientific understanding that information is tangible once recorded.[253] An online course in data science may silence the objections of critics arguing on the grounds of the intangible nature of data. Though accepting the tangible nature of personal data would be useful in understanding that personal data is property, it is not necessary. Property includes not only tangible possessions but intangible possessions as well.[254]

A second philosophical objection may be raised because more than one person can possess data at the same time. But, as noted above, complete ownership and exclusive control are not necessarily required for Fourth Amendment protection under a property-based approach.[255] Justice Gorsuch raised this point in his dissenting opinion in *Carpenter*.[256] When an individual rents a home, rather than owning it in fee simple, the Fourth Amendment still protects that home from unreasonable search and seizure.[257] Further, multiple individuals may share ownership in a home, and each is entitled to Fourth Amendment protection.

A third philosophical objection is likely to be that even if personal data is property, it should belong to the person or entity that creates the data, rather than the individual to whom the information pertains. While this argument has the support of the historic labor-based theories of property, personal data is unique to modern times. It is unclear if property would have been so defined if expansive digitized records relating to individuals' identities were available long ago. Germany's Federal Minister of Transport and Digital Infrastructure has recognized this fact in proposing a law that makes data legally equivalent to other commodities.[258] Among the principles that this law relies on are notions that "data should belong to the person to which the data pertains," "public data is to be considered as open data," and individuals should be able to make informed decisions regarding the use of their data.[259] The

253 *See* Ritter & Mayer, *supra* note 87, at 223 ("the scientific consensus [is] that digital information is not intangible, but is physical, tangible matter"); *see also id.* at 256 ("[T]he physical quality of information, and the idea that information is a physical constituent of the universe, are widely adopted within the scientific community.").

254 Brandeis & Warren, *supra* note 159, at 193.

255 *See* United States v. Carpenter, 138 S. Ct. 2206, 2269 (2018).

256 *Id*.

257 *Id.* at 2269–70.

258 Ritter & Mayer, *supra* note 87, at 229–30.

259 *Id.*

United States would be wise to adopt this principle, as it best protects the intimate relationship between an individual and his or her personal data.

B. *Consequences of Treating Data as Property Against Private Actors*

As to the business organizations that are likely to kick and scream if property status works its way into the civil law against private actors, arguing that compliance is not feasible, the most straightforward response is that it is not that hard to delete data. By deleting information, a business ensures it is not infringing on property rights that exclude unwanted possession, use, or interference. While it is true that there may be a period that businesses need to expend significant funds in order to become compliant with new laws regulating data as property, this is no reason to abandon the protection that justice requires for personal data.

If personal data were treated as property under a civil statute against private actors, individuals claiming an injury of their rights would be likely to proceed for injunctive relief.[260] Generally, a violation of property rights is remediated by injunction, where a violation of a privacy right is remediated by money damages.[261] This may pose a difficulty, as an injunction must be capable of precise definition in order to be effective.[262] Consider the expansive definition of personal information present in the CCPA.[263] How far would an injunction need to reach in the case of probabilistic identifiers? Would all data that led to identification of the individual need to be included in the injunction? Would it suffice to eliminate just enough information to decrease the probability of identifying the individual? If so, what information should be deleted? Who gets to decide? This trouble with applying injunctive relief presents itself in patent litigation.[264] The difficulty in limiting the scope of the injunction to the asserted property interest leads to situations that "systematically overcompensate plaintiffs and overdeter defendants, with significant negative consequences for innovation and economic growth."[265]

---

[260] *Id.* at 249 (quoting Lemley & Weiser, *supra* note 179, at 786) ("[A] property rule provides for an injunction and a liability rule provides for nonconsensual access in return for a payment of money damages.").

[261] Lemley & Weiser, *supra* note 179, at 786.

[262] *Id.* at 794.

[263] CAL. CIVIL CODE § 1798.140(o)(1) (West 2020).

[264] Lemley & Weiser, *supra* note 179, at 784–85.

[265] *Id.* at 785.

Perhaps there is a way around this, but perhaps this difficulty is unavoidable. Though the Court likely ought to forge ahead and declare that personal data is property subject to Fourth Amendment protection, states may best be left to experiment behind the veil of their legal fiction. By persisting in regulating under privacy law while granting piecemeal property rights to individuals in their personal data, courts will not have to face the difficulties that arise in attempts to fashion appropriate injunctive relief.

C. *Personal Data During a Pandemic*

In late 2019, the COVID-19 pandemic struck the globe and quickly became known as "an unprecedented situation" as a host of novel issues arose.[266] The rapid spread of the coronavirus presented a challenge to concerns over personal data protections. Technology could give governments the ability to stop the spread of COVID-19 by tapping into personal data revealing whom individuals come into contact with or monitoring adherence to stay-at-home orders. But depending on the technology adopted, individuals' rights could be compromised.

Several governments around the world implemented contact tracing technology to contain the pandemic.[267] Some technologies employ Bluetooth to detect individuals' proximity to each other, providing information on when someone contacted a person carrying the coronavirus.[268] These technologies fall on the less invasive end of the spectrum because they do not actually reveal an individual's location. Other technologies rely on GPS tracking[269]—creating the possibility of government access to the location data Supreme Court Justices have recognized could compromise individuals' reasonable expectations of privacy.[270]

---

[266] *See, e.g.*, Bibiana Campos Seijo, *An Unprecedented Situation*, C&EN, Vol. 98, Issue 11 (Mar. 21, 2020), https://cen.acs.org/biological-chemistry/infectious-disease/unprecedented-situation/98/i11; Tyler Thrasher, *Amid Protests and COVID-19, GRTC 'Operating in an Unprecedented Situation*,' ABC 8 NEWS (updated June 3, 2020, 5:21 pm), https://www.wric.com/news/local-news/richmond/amid-protests-and-covid-19-grtc-operating-in-an-unprecedented-situation.

[267] Luke Dembosky, et al., *Can Contact Tracing Apps Help Get Many of Us Back to Work Soon? A Framework for Evaluating the Various Options and Legal Concerns*, DEBEVOISE IN DEPTH: CORONAVIRUS RESOURCE CENTER (Apr. 24, 2020), https://www.debevoise.com/insights/publications/2020/04/can-contact-tracing-apps-help ("China, Hong Kong, Israel, Singapore, South Korea and Taiwan have all had varying degrees of success in using electronic contact tracing . . . to allow a significant portion of their population to return to school and work, albeit with limitations.").

[268] *Id.*

[269] *Id.*

[270] Freiwald & Smith, *supra* note 24, at 216–17 (long-term GPS monitoring).

Concerns amplify if the technology allows for real-time collection of data. This would create the equivalent of wiretapping a conversation in the context of ongoing, immediate access to citizens' locations. For law enforcement to acquire information through a wiretap, officers must make a greater showing than needed for a typical warrant—demonstrating the sensitive nature of intercepting real-time information.[271] Real-time access to individuals' locations would be alarmingly invasive.

If personal data were recognized as property, any government-imposed location tracking would run head-on into Fourth Amendment protections. Despite the grave nature of the pandemic, the United States government did not impose mandatory tracking via GPS technologies. Institutions, such as college universities, by and large, opted for less invasive contact tracing devices, such as those relying on self-reporting of symptoms and Bluetooth technology. Those that did choose to mandate the use of a contact tracing app with GPS monitoring capabilities were met with backlash.[272] Could this be evidence that personal data is already property in the minds of American citizens? Certainly, it lends support to that conclusion.

VII. CONCLUSION

Personal data is gaining momentum on a path toward personal property status. Legislatures are treating personal data as personal property. Individuals are demanding and receiving control of their data as if it were their property. The day may not be far off when the Court recognizes personal data as personal property—an "effect" falling squarely within the Fourth Amendment's protections. While useful, the legal fictions that create difficulties in administrating the law and risk leaving the vulnerable without protection would no longer be necessary. The Court could recognize that personal data is implicitly treated as personal property under state legislation and hold that personal data is an effect under the Fourth Amendment. Doing so would harmonize the original intent to protect effects under the Fourth

---

271 *See* Professor David W. Opderbeck, *Cybersurveillance Developments*, THE CYBERSECURITY LAWYER (June 10, 2016), https://thecybersecuritylawyer.com/2016/06/10/cybersurveillance-developments ("For communications in transit, the Wiretap Act requires a showing of probable cause *plus* a showing that 'normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous.' 18 U.S.C. § 2518(3)." (emphasis added)).

272 *See, e.g.*, Zack Whittaker, *Fearing Coronavirus, A Michigan College is Tracking Its Students with a Flawed App: And Students Have No Way to Opt Out*, TECHCRUNCH (Aug. 19, 2020, 4:30 p.m.), https://techcrunch.com/2020/08/19/coronavirus-albion-security-flaws-app.

Amendment with the emergence of a novel form of personal property—personal data. While remaining useful in other contexts, legal fictions would no longer be needed to protect personal data from unreasonable search and seizure.