PROPERTY RIGHTS OVER PERSONAL DATA: AN ALTERNATIVE FOR STANDING IN DATA BREACH CASES

Plaintiffs seeking to redress injuries resulting from data breaches have received unequal responses when trying to have their day in court. Some federal circuit courts have granted them standing while others have not. Complainants must establish that they have suffered an actual or threatened injury that affects them personally and that the public at large does not share. Courts differ in their decision to grant standing depending on whether plaintiffs have established a concrete enough injury. Some courts deny standing in data breach cases because they consider that the injury alleged is too attenuated. This Comment proposes the bailment theory to data breach cases as an alternative to overcome the existing circuit split. Under the bailment theory, when consumers entrust companies with their personal data they create a bailment. A data breach that exposes consumer data would constitute a breach of the bailment and fulfill the injury requirement to establish standing.

Although some plaintiffs have presented a theory to standing based on bailments, none of their claims have had enough strength. While some courts have bypassed the argument, others have rejected it based on substantive grounds. Courts have rejected the bailment theory on the following premises: the parties did not meet one of the elements of a bailment, the company entrusted with the data did not participate actively in the breach, or the personal data was not considered to be a form of property. This Comment presents recommendations to increase the strength of breach of bailment arguments in data breach cases as an alternative to obtain standing.

TABLE OF CONTENTS

I. INTRODUCTION

Your data is valuable to *you* regardless of the context in which it is used. The value you assign to your data can stem from an emotional source, from the fact that you want to keep it secret, or even from its monetary worth as a tradeable asset.[1] Beyond how you value your data, companies can profit from it and use it to provide new and better services.[2] Put differently, your personal data can be a product that generates profit.[3]

When you entrust your personal data to a company that will provide you with a good or service, you expect them to safeguard your data;[4] however, in increasing numbers, that is not the case.[5] Cybercriminals launch attacks against companies that hold bulks of personal data. They operate by infiltrating a data source and extracting sensitive information; this is known as a data breach—whether it is done physically or remotely by bypassing the company's

1. *See* Sarah Spiekermann et al., *The Challenges of Personal Data Markets and Privacy*, 25 ELEC. MKTS. 161, 161 (2015).

2. *Id.*

3. *Id.*

4. *See 81% of Consumers Would Stop Engaging with a Brand Online After a Data Breach, Reports Ping Identity*, BUS. WIRE (Oct. 22, 2019, 8:00 AM), https://www.businesswire.com/news/home/20191022005072/en/81-Consumers-Stop-Engaging-Brand-Online-Data.

5. Nicole Martin, *What Is a Data Breach?*, FORBES (Feb. 25, 2019, 12:27 PM), https://www.forbes.com/sites/nicolemartin1/2019/02/25/what-is-a-data-breach/#31cec3e214bb.

network security.[6] Many companies have been targeted by these attacks to extract a wide range of data that comprises addresses, social security numbers, financial information, health information, phone numbers, names, and other sensitive data.[7]

This scenario is not far-fetched or surreal: in only the first six months of 2019, there were more than 3,800 publicly disclosed breaches exposing 4.1 billion records, 3.2 billion of which were exposed in just eight breaches.[8] However, these are just a fraction of the 38 billion records exposed in at least 40,650 breaches in the last decade.[9] Some of the companies targeted by the largest data breaches of the decade include MyFitnessPal (143.6 million records hacked), Equifax (147 million records hacked), Exactis (340 million records hacked), Marriott (383 million records hacked), River City Media (1.37 billion records hacked), and the largest data breach to date, Yahoo! (3 billion records hacked).[10] Many other companies have been affected.[11]

Companies hold a wide spectrum of consumer data that is at risk of a latent threat of exposure. In early 2020, the Peekaboo Moments app, which provides services related to tracking a baby's growth through the storage of audiovisual materials,[12] left unsecured thousands of baby photos and videos, as well as device data and email addresses.[13] In another data breach, 1.2 million user profiles from

---

6. *Data Breaches 101: How They Happen, What Gets Stolen, and Where It All Goes*, TREND MICRO (Aug. 10, 2018), https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101.

7. *Id.*

8. Davey Winder, *Data Breaches Expose 4.1 Billion Records in First Six Months of 2019*, FORBES (Aug. 20, 2019, 6:31 AM), https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/#735a95abd549.

9. Megan Leonhardt, *The 10 Biggest Data Hacks of the Decade*, CNBC MAKE IT (Dec. 27, 2019, 9:01 AM), https://www.cnbc.com/2019/12/23/the-10-biggest-data-hacks-of-the-decade.html.

10. *Id.*

11. *See* Daniel Funke, *By the Numbers: How Common are Data Breaches — and What Can You Do About Them*?, POLITIFACT: NAT'L (Sept. 23, 2019), https://www.politifact.com/article/2019/sep/23/numbers-how-common-are-data-breaches-and-what-can-/; Aaron Holmes, *The Biggest Hacks of 2019 So Far*, BUS. INSIDER (Sept. 11, 2019, 12:32 PM), https://www.businessinsider.com/biggest-hacks-and-data-breaches-of-2019-capital-one-whatsapp-iphone-2019-9; Leonhardt, *supra* note 9; David Murphy, *The Worst Data Breaches of 2019*, LIFE HACKER (Dec. 26, 2019, 10:00 AM), https://lifehacker.com/the-worst-data-breaches-of-2019-1840616463.

12. *About Us*, PEEKABOO MOMENTS, https://peekaboomoments.com/about (last visited Apr. 28, 2021).

13. Jeremy Kirk, *Baby's First Data Breach: App Exposes Baby Photos, Videos*, BANK INFO SEC. (Jan. 14, 2020), https://www.bankinfosecurity.com/babys-first-breach-app-exposes-baby-photos-videos-a-13603.

the Luscious porn website were exposed.[14] Users gathered on Luscious to anonymously share and comment on Japanese cartoon porn known as *hentai*.[15] The data exposed included usernames, personal email addresses (some of which revealed the users' full names), user activity log, location, and gender.[16]

Now think about the extent of technology's involvement in your daily life and how often you give others your data. You might give your data to an array of apps in order to have access to transportation, file storage, grocery delivery, financial management, language learning, email services, health and fitness tracking, social media, online shopping, dating, chatting, etc. Even if not provided through a digital platform, you also give away your data when you visit the doctor's office, ask for a loan, open a bank account, or get a new credit card. What options does a consumer have to vindicate his rights when his data becomes compromised?

The first thought that might come to mind is suing the company that did not protect the data, but this may pose a challenge to potential plaintiffs. Plaintiffs must show they have standing to sue the company that held their data.[17] Under the current circuit split on the issue of standing in data breach cases, the plaintiffs' success will depend on the jurisdiction where they file their complaint and on whether the hacker used their data.[18] Some jurisdictions find that standing is justified because the exposure of data after a breach creates a concrete enough risk of harm.[19] On the contrary, other jurisdictions require a more concrete financial harm because the risk of future harm created by the breach is too attenuated.[20]

One alternative to this heterogeneous treatment of the issue is applying the bailment theory to standing in data breach cases. Under this theory, when consumers share their personal data with companies that will render them goods or services, a bailment comes to life.[21] The breach of this relationship, regardless of a hacker's potential use of the data, inflicts an injury on the consumer.[22] This Comment proposes to revitalize the idea of bailments to maintain them as part of our legal system, explores courts' arguments against

---

14. Davey Winder, *Popular Porn Site Breach Exposed 1.2 Million 'Anonymous' User Profiles*, FORBES (Aug. 20, 2019, 2:58 AM), https://www.forbes.com/sites/daveywinder/2019/08/20/popular-porn-site-breach-exposed-12-million-anonymous-user-profiles/#4c61cc577039.

15. *Id.*

16. *Id.*

17. *See* discussion *infra* Subparts II.B, II.C.

18. *See* discussion *infra* Subparts II.B, II.C.

19. *See* discussion *infra* Subpart II.C.2.

20. *See* discussion *infra* Subpart II.C.3.

21. *See* discussion *infra* Subparts II.D, III.B.

22. *See* discussion *infra* Subparts II.D, III.B.

bailments in personal data, and presents counterarguments to the apparent deficiencies in the bailment theory.

This Comment starts with a basic hypothetical around which the arguments presented will center. Then, this Comment will succinctly outline the constitutional requirements for standing and courts' prevailing postures regarding standing in data breach cases. Next, this Comment will explore the elements of and conceptions about bailments. Then, this Comment presents a discussion about why bailments arise when a company holds consumer data and includes a discussion about personal data being subject to property rights. Last, this Comment introduces some arguments that could make bailment claims in data breach cases more successful.

II. BACKGROUND

A. The Basic Hypothetical

The scenario that this Comment addresses is that of a data breach perpetrated against a private company.[23] For example, Consumer A registers for a service with Company B and provides his full name, date of birth, address, credit card information, phone number, and email address, among other data. Consumer A and Company B might have agreed to the terms controlling their relationship in a contract. Additionally, there is no waiver of liability that would be applicable in the event of a potential lawsuit based on a breach of bailment.

Consumer A successfully uses the service while thinking that his data is safe in the hands of Company B. At a later date, hackers unlawfully obtain the bulk of consumer data within Company B's systems. The hackers might have obtained the consumer data either because they launched an attack against Company B's systems or because Company B exposed the data, making the hackers' goal easier to attain. Regardless of whether the hackers have used, are using, or plan to use the data obtained, they have obtained Consumer A's data.

This is the hypothetical around which arguments in favor of granting standing will follow. It will not matter for finding standing under the bailment theory whether or not the hackers in fact have used, are using, or plan to use Consumer A's data. Under the

23. The core of this Comment is not the use of data by its original collector. It is not centered in a scenario where a company *itself* uses the data a consumer has provided or the company has collected within the scope of its relationship with the consumer. That would leave out of the reach of this Comment the ethical implications of using data to prompt ads that are tailored to the needs and characteristics of a consumer or selling data to a third party with the consent of consumers (or not). Furthermore, this Comment does not address data breaches that penetrate government databases—that scenario could present a diverse range of implications that this Comment will not cover.

bailment theory, there should be no difference for standing purposes between Consumer A, whose data has not been used and who lacks knowledge about whether the hackers would ever use his data, and Consumer C, who has evidence of suspicious credit card activity traceable to the breach. Although the likelihood of establishing an injury under the current circuit split varies across jurisdictions,[24] under the bailment theory, both Consumer A and Consumer C would have suffered an injury in fact.

B. The Constitutional Requirement of Standing

Standing is a constitutional restriction to the exercise of the judicial power,[25] which "shall extend to all Cases [and] . . . Controversies."[26] The Supreme Court has explained that a citizen's general interest in an issue is not enough to convey standing; the alleged injury cannot be indefinite and shared with people in general.[27] The plaintiff must show a direct injury or that he is in immediate danger of suffering a direct injury as a result of the actions of the party against whom he is taking judicial action.[28] The core of the standing question is whether the plaintiff is the proper party to bring this particular case because he has alleged a personal stake in its outcome.[29] In order to demonstrate standing, the complainant must establish: (1) an actual or threatened injury that is not a generalized grievance shared by a large number of people, (2) such an injury was a consequence of the defendant's unlawful activities, and (3) a favorable judicial decision will likely redress the harm.[30]

The standing requirement for a personalized, actual injury demands that the injury be distinct from those common to people in general and palpable, not hypothetical.[31] The injury suffered by the complaining party cannot be too abstract, too attenuated in its causal connection to the defendant, or too speculative in its chances of obtaining relief from a favorable judicial decision.[32] Moreover, the standing requirements can be met even if the complaining party has

---

24. *See In re* Zappos.com, Inc., 888 F.3d 1020 (9th Cir. 2018); Attias v. Carefirst, Inc., 865 F.3d 620 (D.C. Cir. 2017); Whalen v. Michaels Stores, Inc., 689 F. App'x 89 (2d Cir. 2017); Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017); *In re* Supervalu, Inc., 870 F.3d 763 (8th Cir. 2017); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384 (6th Cir. 2016); Remijas v. Neiman Marcus Grp., 794 F.3d 688 (7th Cir. 2015).

25. Flast v. Cohen, 392 U.S. 83, 94 (1968).

26. U.S. CONST. art. III, § 2.

27. Massachusetts v. Mellon, 262 U.S. 447, 488 (1923); Fairchild v. Hughes, 258 U.S. 126, 129–30 (1922).

28. *Mellon*, 262 U.S. at 488.

29. *Flast*, 392 U.S. at 99–100.

30. Lujan v. Defs. of Wildlife, 504 U.S. 555, 560–61 (1992); Warth v. Seldin, 422 U.S. 490, 499, 501, 505 (1975).

31. Allen v. Wright, 468 U.S. 737, 752 (1984).

32. *Id.*

not yet suffered the harm, although the complaining party has the burden of establishing that the harm is imminent.[33] For example, a description of an injury that references some future day, without any concrete details or specifications, will not be considered imminent enough.[34] Besides the limitation that standing exerts on the exercise of judicial power,[35] it also serves to contain the flow of litigants that otherwise have no personal stake in litigation—standing creates a door that prevents too many cases from entering courts.[36]

C. How Courts Determine if a Data Breach Case Has Standing

Data breaches pose a complicated fact pattern in which to apply the basic notions of the standing doctrine.[37] In data breach cases, whether or not a plaintiff has standing usually turns on the first prong—an actual injury.[38] A plaintiff that establishes that he has suffered an actual or threatened injury in fact as a result of a data breach is more likely to succeed than one that cannot meet that threshold.[39]

Although the Supreme Court has touched on the issue of standing in cases where personal data is key, it has not yet addressed the core of the query in data breach cases.[40] That is why circuit courts have developed diverse responses to the question of standing in data breach cases.[41] When the plaintiff's stolen data has been used for fraudulent purposes, courts usually find that there is standing because the plaintiff has suffered a particularized injury that could take the form of a monetary loss.[42] On the other hand, when the plaintiff's data has been stolen but there is no indication that the data's unlawful possessor has used it in a fraudulent way, courts disagree on whether the first prong to establish standing has been

---

33. *Lujan*, 504 U.S. at 560–64.

34. *Id.* at 563–64.

35. Flast v. Cohen, 392 U.S. 83, 94 (1968).

36. *Allen*, 468 U.S. at 755–56.

37. Amanda Lawrence et al., *The Great Data Breach Standing Circuit Split*, LAW360 (Jan. 25, 2019, 3:29 PM), https://www.law360.com/articles/1121370/the-great-data-breach-standing-circuit-split.

38. *See id.*

39. *See In re* Supervalu, Inc., 870 F.3d 763, 768–74 (8th Cir. 2017).

40. Frank v. Gaos, 139 S. Ct. 1041, 1043–46 (2019); Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1544–50 (2016); Clapper v. Amnesty Int'l USA, 568 U.S. 398, 408–22 (2013).

41. *See In re* Zappos.com, Inc., 888 F.3d 1020, 1023–30 (9th Cir. 2018); In re *Supervalu, Inc.*, 870 F.3d at 766–74; Attias v. Carefirst, Inc., 865 F.3d 620, 624–30 (D.C. Cir. 2017); Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90–91 (2d Cir. 2017); Beck v. McDonald, 848 F.3d 262, 267–77 (4th Cir. 2017); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 385, 387–91 (6th Cir. 2016); Remijas v. Neiman Marcus Grp., 794 F.3d 688, 690–97 (7th Cir. 2015).

42. *See* In re *Supervalu, Inc.*, 870 F.3d at 772–74.

satisfied.[43] Thus, under the current circuit split, whether or not a plaintiff meets the standing threshold is dependent on a court's perception about how concrete the likelihood of fraudulent use of the data is.[44]

1. The Supreme Court

The Supreme Court has addressed the question of standing in cases relating to personal data.[45] In *Clapper v. Amnesty International USA*,[46] the plaintiffs asserted a statutory cause of action against the use of government surveillance to track third parties.[47] The plaintiffs argued that they had standing because there was an objectively reasonable likelihood that their data would be acquired by the government.[48] While *Clapper* does not deal with the scenario studied in this Comment,[49] this case is important because the Court indicated an injury must be "concrete, particularized, and actual or imminent" to be the source of standing.[50] The Court further clarified that a "threatened injury must be certainly impending to constitute injury in fact."[51] The Court rejected plaintiffs' standing theory because it was too speculative and relied on an attenuated chain of possibilities.[52] The opinion also contained an alternative standard where standing is found if there is a substantial risk that harm will occur.[53] Although the Court did not explain the reach of this standard, it determined that the plaintiffs also failed to meet that threshold.[54]

Further, in *Spokeo, Inc. v. Robins*,[55] while not a data breach case, the Court gave additional information about the standard a plaintiff

43. *See* In re *Zappos.com, Inc.*, 888 F.3d at 1023–24, 1027–29; In re *Supervalu, Inc.*, 870 F.3d at 768–72; *Attias*, 865 F.3d at 625–29; *Whalen*, 689 F. App'x at 90–91; *Beck*, 848 F.3d at 270–77; *Galaria*, 663 F. App'x at 385, 387–89; *Remijas*, 794 F.3d at 692–94.

44. *See* In re *Zappos.com, Inc.*, 888 F.3d at 1023–24, 1027–29; In re *Supervalu, Inc.*, 870 F.3d at 768–72; *Attias*, 865 F.3d at 625–29; *Whalen*, 689 F. App'x at 90–91; *Beck*, 848 F.3d at 270–77; *Galaria*, 663 F. App'x at 385, 387–89; *Remijas*, 794 F.3d at 692–94.

45. *Frank*, 139 S. Ct. at 1043–44; *Spokeo, Inc.*, 136 S. Ct. at 1544; *Clapper*, 568 U.S. at 401.

46. 568 U.S. 398 (2013).

47. *Id.* at 401.

48. *Id.*

49. *See supra* Subpart II.A.

50. *See Clapper*, 568 U.S. at 409.

51. *Id.* (emphasis omitted).

52. *Id.* at 410–14.

53. *See id.* at 414 n.5; Michael Hopkins, Comment, *Your Personal Information Was Stolen? That's an Injury: Article III Standing in the Context of Data Breaches*, 50 U. PAC. L. REV. 427, 437 (2019).

54. *See Clapper*, 568 U.S. at 414 n.5.

55. 136 S. Ct. 1540 (2016).

must meet to have standing.[56] The plaintiff in *Spokeo* presented a statutory claim against a website operator who ran a "people search engine" for disseminating inaccurate data about the plaintiff.[57] The Court reversed the circuit court's decision granting the plaintiff standing because the Ninth Circuit failed to distinguish between the requirements that the injury be both particularized and concrete.[58] The Court stated that a particularized injury is one that affects the plaintiff in a personal and individual way, while on the other hand, a concrete injury is one that in fact exists.[59]

While these decisions shed light on what constitutes an injury for standing purposes, they still do not address the specific question of standing in a data breach.[60] Moreover, these decisions do not clarify how to apply their legal frameworks in a concrete way, leaving that decision to the circuit courts.[61] Thus, the circuit split on standing in data breach cases continues. In the next Subparts, this Comment analyzes the circuit split after the *Clapper* and *Spokeo* decisions.

2. Pro–Standing Circuits

Circuits finding standing in data breach cases include the D.C., Sixth, Seventh, and Ninth Circuits.[62] These courts have held that the exposure of a plaintiff's data increases his risk of suffering future harm stemming from the data breach.[63] These courts may find standing based on the mere fact of the breach because they consider that the risk of future injury is sufficiently concrete.[64]

In *Attias v. Carefirst, Inc.*,[65] a lawsuit was filed against a health insurance company after a data breach in which customer data was stolen.[66] The D.C. Circuit found that plaintiffs had standing because plaintiffs had a plausible allegation of a substantial risk of identity theft.[67] The fact that an unauthorized third party targeted and actually accessed their data made the plaintiffs' claim less speculative and suggested that the hacker had the intent and ability to use their

---

56. *See id.* at 1548–50.
57. *Id.* at 1544–46.
58. *Id.* at 1550.
59. *Id.* at 1548.
60. *See id.* at 1544–50; Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401–22 (2013).
61. *See Spokeo, Inc.*, 136 S. Ct. at 1544–50; *Clapper*, 568 U.S. at 401–22.
62. *See In re* Zappos.com, Inc., 888 F.3d 1020, 1023, 1027–30 (9th Cir. 2018); Attias v. Carefirst, Inc., 865 F.3d 620, 622, 627–30 (D.C. Cir. 2017); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 385, 388, 390–91 (6th Cir. 2016); Remijas v. Neiman Marcus Grp., 794 F.3d 688, 689–90, 697 (7th Cir. 2015).
63. Lawrence et al., *supra* note 37; *see* cases cited *supra* note 62.
64. Lawrence et al., *supra* note 37; *see* cases cited *supra* note 62.
65. 865 F.3d 620 (D.C. Cir. 2017).
66. *Id.* at 622.
67. *Id.* at 628.

data for ill.[68] The mere hack and theft of personally identifiable data created a substantial risk of harm.[69]

The Seventh Circuit also favored standing in data breach cases in *Remijas v. Neiman Marcus Group, LLC*.[70] In that case, a data breach exposed the plaintiffs' credit card information held by the defendant.[71] Among other claims, the plaintiffs argued that they had "an increased risk of future fraudulent charges and greater susceptibility to identity theft."[72] The court decided that such an imminent injury was enough to show a substantial risk of harm given that the plaintiffs' data had been targeted by the perpetrators, and it could be presumed that the hackers' goal was to eventually use the data for fraudulent purposes.[73]

Standing was also favored by the Ninth Circuit in *In re Zappos.com, Inc.*[74] This case was brought by plaintiffs whose personal data had not yet been used to commit fraud.[75] Like in other cases in this Subpart, the court found that the personal data stolen in the data breach—which included credit card information—could be used to commit identity theft or identity fraud.[76] That threat was sufficient to allege a substantial risk of suffering an injury in fact.[77]

The Sixth Circuit has also conferred standing to plaintiffs in data breach cases.[78] A case from this circuit favoring standing is *Galaria v. Nationwide Mutual Insurance Co.*,[79] which is discussed in Subpart III.B.1 of this Comment.[80]

3. Adverse–to–Standing Circuits

Contrary to the circuits discussed above, the Second, Fourth, and Eighth Circuits have found no standing in data breach cases.[81] Typically, these circuits require a more concrete financial harm to find standing.[82] Therefore, the increased risk of future harm to which

68. *Id.* at 628–29.
69. *Id.* at 629.
70. 794 F.3d 688 (7th Cir. 2015).
71. *Id.* at 689–90.
72. *Id.* at 692.
73. *Id.* at 693.
74. 888 F.3d 1020 (9th Cir. 2018).
75. *Id.* at 1023.
76. *Id.* at 1023, 1028.
77. *Id.* at 1029.
78. Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 384–91 (6th Cir. 2016).
79. 663 F. App'x 384 (6th Cir. 2016).
80. *See infra* Subpart III.B.1.
81. *See In re* Supervalu, Inc., 870 F.3d 763, 763–74 (8th Cir. 2017); Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 89–91 (2d Cir. 2017); Beck v. McDonald, 848 F.3d 262, 262–78 (4th Cir. 2017).
82. *See* In re *Supervalu, Inc.*, 870 F.3d at 763–74; *Whalen*, 689 F. App'x at 89–91; *Beck*, 848 F.3d at 262–78; Lawrence et al., *supra* note 37.

a victim of a data breach is exposed is not enough to have standing in these circuits.[83] For these courts, the risk of future injury is too attenuated to find standing.[84] The nature of the information breached also informs how courts rule in these circuits.[85]

In *Whalen v. Michaels Stores, Inc.*,[86] the Second Circuit affirmed a district court decision finding no standing where the plaintiff's credit card information was exposed after a data breach.[87] Using *Clapper* as a foundation, the Second Circuit found no standing where the plaintiff alleged that after the breach, a third party attempted to use her stolen credit card information twice—but no purchases were made—and she faced a risk of future identity fraud.[88] The Second Circuit ruled that the plaintiff had not alleged any injury that would satisfy standing because she did not have to pay for any fraudulent charges and did not face any risk of future fraud given that her credit card was canceled.[89]

Another example is *Beck v. McDonald*,[90] which involves a data breach perpetrated against a government agency and illustrates the Fourth Circuit's position with respect to data breaches.[91] Applying the standard outlined in *Clapper*, the Fourth Circuit decided that an alleged increased risk of future identity theft did not suffice to find that the threat was sufficiently imminent, and thus, was not certainly impending.[92] In this case, items containing personal data were stolen. However, that mere fact was insufficient to find that the thief's goal was to obtain the data where evidence indicating that the data was accessed or misused was missing.[93] Moreover, even though the plaintiffs presented statistics about the use of stolen data in health-related breaches, the court deemed those insufficient to establish a substantial risk of harm.[94]

Finally, in *In re Supervalu, Inc.*,[95] the defendants' grocery stores were attacked by hackers that obtained consumer credit card information.[96] Out of the sixteen plaintiffs in the case, only one alleged that he noticed a fraudulent charge on his credit card

83. *See* In re *Supervalu, Inc.*, 870 F.3d at 763–74; *Whalen*, 689 F. App'x at 89–91; *Beck*, 848 F.3d at 262–78; Lawrence et al., *supra* note 37.

84. *See* In re *Supervalu, Inc.*, 870 F.3d at 763–74; *Whalen*, 689 F. App'x at 89–91; *Beck*, 848 F.3d at 262–78; Lawrence et al., *supra* note 37.

85. *See* In re *Supervalu, Inc.*, 870 F.3d at 770–71.

86. 689 F. App'x 89 (2d Cir. 2017).

87. *Id.*

88. *Id.* at 90.

89. *Id.* at 90–91.

90. 848 F.3d 262 (4th Cir. 2017).

91. *Id.* at 267.

92. *Id.* at 275–76.

93. *Id.* at 274–75.

94. *Id.* at 275–76.

95. 870 F.3d 763 (8th Cir. 2017).

96. *Id.* at 765.

statement.[97] The court granted that specific plaintiff standing because the fraudulent charge to his credit card constituted a present injury in fact.[98] On the other hand, the remaining fifteen plaintiffs only alleged that they were under an "imminent and real possibility of identity theft."[99] The court ruled that these remaining plaintiffs did not have a substantial risk of suffering an injury because the nature of the stolen data—which did not include any personally identifiable information—did not enable identity theft.[100] The ruling was also influenced by the evidence plaintiffs presented to support their assertion that data breaches facilitate identity theft—the United States Government Accountability Office ("GAO") report on data breaches—which also indicated that most breaches are unlikely to result in fraud.[101]

D. The Bailment Theory for Standing in Data Breach Cases

Courts state with varying language the standard that gives rise to bailments. Bailments are created by the "delivery of personal property from one person to another for a specific purpose" where such delivery is accepted in conjunction with the understanding that the property would be disposed of at the owner's directions and that the purpose underlying the bailment will be completed.[102] The parties may also be required to intend to create a bailment.[103] However, there is no need to enter a formal contract reflecting these elements.[104] Even where the parties have not met all the elements, courts may imply the existence of a bailment as long as lawful possession exists.[105] An alleged bailee has lawful possession over property when he has both physical control and an intent to exercise that control over the bailed property.[106]

Alternatively, a bailment can be defined as an

> agreement, either *express* or *implied*, [where] one person . . . entrust[s] personal property to another for a specific purpose and . . . [after accomplishing such] purpose . . . , the bailee will return the property to the bailor[,] . . . deal with it

97. *Id.* at 767.
98. *Id.* at 772–74.
99. *Id.* at 766.
100. *Id.* at 770.
101. *Id.* at 770–71.
102. State v. Johnson, 326 P.3d 361, 364 (Idaho Ct. App. 2014); *see* Waugh v. Univ. of Haw., 621 P.2d 957, 968 (Haw. 1980); 8 C.J.S. *Bailments* § 18 (2020).
103. *Waugh*, 621 P.2d at 968.
104. Morris v. Hamilton, 302 S.E.2d 51, 52 (Va. 1983).
105. *Waugh*, 621 P.2d at 969; *Morris*, 302 S.E.2d at 53.
106. *Morris*, 302 S.E.2d at 53.

> according to the bailor's directions, or keep it until the bailor reclaims it.[107]

Under the bailment theory, consumers entrust their personal data to companies in order to enable the latter to render services.

It is plausible to argue that a bailment is created when the bailor (the individual) delivers his property to the bailee (the company) and the company accepts the property.[108] The element of delivery is met when the property is put in the bailee's possession so as to exclude all others and give the bailee the sole custody and control of the property.[109] Here, the consumer puts his personal data in the company's control, but it is merely a copy of the information which still remains within the consumer's knowledge. However, the copy the company retains is likely beyond the consumer's reach.[110] Furthermore, under some definitions of a bailment, the legal standard is also met when someone other than the owner has rightful possession of goods and an express or implied mutual agreement to safely keep the goods.[111] The bailee must accept the property either under a contract or under circumstances that imply its existence.[112] The bailee then exercises complete dominion at all times over the goods and is under a duty to return those goods once the purpose of the bailment is accomplished.[113]

Some companies have included contract terms about the data's final treatment,[114] which would be in accordance with establishing a bailment relationship.[115] For example, OnlyFans, a social network

---

107. C.J.S., *supra* note 102, § 1 (emphasis added).

108. *See id.*

109. G. J. C., Annotation, *Bailment: What Amounts to Delivery of, or Assumption of Control Over, Property Essential to a Bailment*, 1 A.L.R. 394 (1919).

110. *See* Natasha Singer & Prashant S. Rao, *U.K. vs. U.S.: How Much of Your Personal Data Can You Get?*, N.Y. TIMES: TECH. (May 20, 2018), https://www.nytimes.com/interactive/2018/05/20/technology/what-data-companies-have-on-you.html (explaining that Americans do not have a right to access their data when held by a company).

111. C.J.S., *supra* note 102, § 1.

112. G. J. C., *supra* note 109.

113. C.J.S., *supra* note 102, § 1.

114. *See* Nerushka Bowan, *Social Media: What Happens When You Delete Your Account?*, NORTON ROSE FULBRIGHT: SOC. MEDIA L. BULL. (June 19, 2014), https://www.socialmedialawbulletin.com/2014/06/social-media-what-happens-when-you-delete-your-account/; Eric Griffith, *How to Delete Your Accounts from the Internet*, PCMAG (Mar. 14, 2017), https://www.pcmag.com/news/how-to-delete-your-accounts-from-the-internet; Lily Hay Newman, *Google Will Delete Your Data by Default—in 18 Months*, WIRED: SEC. (June 24, 2020, 12:36 PM), https://www.wired.com/story/google-auto-delete-data/.

115. Alexa L. Ashworth, Annotation, *Breach of Bailment of Electronic Data*, 91 A.L.R.6th 409 (2014).

that allows users to exchange adult content for money,[116] holds user data for six months after the individual decides to delete his account and only retains the data it needs to comply with government regulations.[117] The data of those deleting Facebook will be held for as long as three months, but after that period, Facebook still retains log data without personally identifiable traits forever.[118] One caveat is that comments made on someone else's posts and posts others shared with your data will not be deleted as long as those individuals do not delete their accounts.[119]

Assuming that courts would deem that in the hypothetical presented in this Comment one or more of the elements of a bailment are missing, a bailment can be implied even where no formal contract exists.[120] The key elements in deciding whether a bailment exists are whether the bailee is in lawful possession of the goods—regardless of how that lawful possession was established—and whether the bailee is accounting for the goods as the property of another.[121] In the case of a bailment in personal data, the data has no physical form but the company has control over its electronic form and intends to exercise that control by excluding all others from the data.[122] Moreover, companies recognize that the data belongs to the individuals as it is their prerogative to decide how to dispose of the data.[123]

An implied-in-law bailment may arise where sufficient circumstances indicate that the relationship between bailor and bailee rests upon a substantive foundation.[124] In some scenarios, the mere fortuitous possession and control of a person's property suffices to create a bailment.[125] One possible circumstance that creates a bailment occurs when a person seeks a company to provide services

116. Jacob Bernstein, *How OnlyFans Changed Sex Work Forever*, N.Y. TIMES (Feb. 9, 2019), https://www.nytimes.com/2019/02/09/style/onlyfans-porn-stars.html.

117. *Privacy Center and Terms: Personal Data*, ONLYFANS, https://onlyfans.com/help/1/11/103 (last visited Apr. 28, 2021).

118. Aimee Picchi, *OK, You've Deleted Facebook, But Is Your Data Still Out There?*, CBS NEWS (Mar. 23, 2018, 5:00 AM), https://www.cbsnews.com/news/ok-youve-deleted-facebook-but-is-your-data-still-out-there/.

119. *Id.*

120. C.J.S., *supra* note 102, § 1.

121. *See* Fada Indus., Inc. v. Falchi Bldg. Co., 730 N.Y.S.2d 827, 839–40 (N.Y. Sup. Ct. 2001); C.J.S., *supra* note 102, § 3.

122. *See* Singer & Rao, *supra* note 110 (explaining that Americans do not have a right to access their data when held by a company).

123. *See supra* text accompanying notes 112–17.

124. *See* W.E. Stephens Mfg. Co. v. Goldberg, 225 S.W.3d 77, 80–81 (Tex. App. 2005).

125. Morris v. Hamilton, 302 S.E.2d 51, 52–53 (Va. 1983).

with respect to the bailed property even where no instructions about the disposition of the property exist.[126]

The bailment theory for standing in data breach cases proposes that where a consumer delivers his personal data to a company that needs such data to render a service or provide a good, a bailment relationship arises. Therefore, when a hacker unlawfully obtains the consumer's data, the consumer suffers an injury in the form of a decrease in value of his data caused by the exposure. For a bailment to exist in this case, personal data must be considered property. Later Parts examine whether personal data could be subject to this treatment.

III. ANALYSIS—AN ALTERNATIVE TO THE CURRENT CIRCUIT SPLIT

A. The Value of Personal Data as Subject to Property Rights

Personal data includes a wide spectrum of information bits: a person's name, social security number, gender, address, appearance, likes, dislikes, financial information, health information, occupation, place and date of birth, education level, household size, relationship status, political and religious affiliations, hobbies, sexual orientation, and any other piece of information disclosed or tracked on the internet.[127] These bits of digital information are like little points over a canvas in a pointillist painting that when seen together, create an image that reflects the person's digital identity.[128] This digital identity, the mass of personal data describing an individual, can be conceived of as property. The following Subparts present legal and normative arguments favoring the existence of property rights over personal data.

1. Legal Conceptions About Property and Personal Data

In the United States, the federal government lacks power to define what constitutes property; the power to create those boundaries resides under state law.[129] Property rights are a

126. Tex. Cap. Bank v. First Am. Title Ins. Co., 822 F. Supp. 2d 678, 683 (W.D. Ky. 2011).

127. *See* Vera Bergelson, *It's Personal But Is It Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379, 381 (2003); Thomas Hemnes, *The Ownership and Exploitation of Personal Identity in the New Media Age*, 12 J. MARSHALL REV. INTELL. PROP. L. 1, 8, 18 (2012).

128. Hemnes, *supra* note 127, at 17.

129. *See* Pruneyard Shopping Ctr. v. Robins, 447 U.S. 74, 84 (1980). However, the federal government has power over what constitutes intellectual property. Yet, personal data is not a trademark because it is not displayed in products to identify the source of the goods, *see* 15 U.S.C. § 1127, and it is not patentable because it is not a novel, useful, and non-obvious invention. *See* 35 U.S.C. §§ 101–03. Personal data is also not subject to copyright law because it is not an original work of authorship within the meaning of the statute. *See* 17 U.S.C. § 102. One

fundamental means to allow individuals to get a hold on their own freedom, plan and shape their destiny, and exercise rights on what is theirs.[130] However, figuring out where to draw the dividing line between what constitutes property and what does not is not a simple endeavor. The legal implications of the word "property" have a comprehensive meaning of the widest significance.[131] Regardless of the difficulties in providing a definition, courts have proposed definitions among which is that the term property "*extends to every species of valuable right and interest, and includes real and personal property*."[132]

This conception of property implies that there is value in the right held over a certain thing and that it is practical to assign a monetary value to it.[133] An individual holding his personal data finds value in his capacity to use it or exclude others from accessing it.[134] The value the individual assigns can be monetary because some people are willing to surrender certain aspects of their privacy in exchange for money—for example, when you provide personal data in a paid scientific study,[135] when a person makes a TV appearance such as on a reality show,[136] or when a celebrity sells their baby's pictures to a magazine.[137] On the other hand, those who want access to the data also assign a monetary value to it.[138] In other words, market forces are at play in assigning a value to personal data through the competing interests of the parties involved.

It is important to remember that the term "property" alludes to not only the physical or abstract object but also to the legal sense of

---

could argue that compilations of personal data are copyrightable, but that protection would only extend to the contributions of the compilation's author.

130. Murr v. Wisconsin, 137 S. Ct. 1933, 1943 (2017).

131. Womack v. Womack, 172 S.W.2d 307, 308 (Tex. 1943); Wells Labberton v. Gen. Cas. Co. of Am., 332 P.2d 250, 254 (Wash. 1958).

132. *Womack*, 172 S.W.2d at 308 (emphasis added).

133. Hildebrand v. S. Bell Tel. & Tel. Co., 14 S.E.2d 252, 256 (N.C. 1941).

134. *See* Hemnes, *supra* note 127, at 7–8.

135. *See How Much Do Research Studies Usually Pay?*, MIA. CLINICAL RSCH.: BLOG (Dec. 20, 2018), https://miamiclinicalresearch.com/how-much-do-research-studies-usually-pay/; Halina Zakowicz, *How to Participate in Paid Clinical Trials in 2021*, IVETRIEDTHAT: SIDE CASH (Nov. 16, 2020), https://ivetriedthat.com/paid-clinical-trials/.

136. *See* Tierney Bricker, *How Much Reality TV Contestants Actually Make (If Anything)*, E! ONLINE (Oct. 11, 2018, 5:15 PM), https://www.eonline.com/news/975767/how-much-reality-tv-contestants-actually-make-if-anything; Kirsten R., *The Secret Paychecks of All Your Favorite Reality TV Stars*, CELEBUZZ (Sept. 3, 2019, 1:17 PM), https://www.celebuzz.com/g/reality-tv-star-salary/ (explaining that profits ranged from millions to nothing). However, those receiving nothing obtained fame, sponsorships, and career opportunities. R., *supra*.

137. *See* Marcus Baram, *Celebs Selling Baby Photos: Expected or Exploitation?*, ABC NEWS (Apr. 14, 2009, 4:07 PM), https://abcnews.go.com/Entertainment/story?id=4318533&page=1.

138. *See* Hemnes, *supra* note 127, at 4, 8.

the word that illustrates the number of rights a person, through his dominion, can exercise over that physical or abstract thing.[139] The aggregation of rights a person or a number of persons can exercise over that which they own is commonly referred to as the bundle of sticks.[140] The bundle of sticks includes rights to exclude, possess, use, enjoy, and dispose of property, be it through modification, destruction, or transfer.[141]

While the law does not generally recognize personal data as subject to property rights,[142] the general conceptions of property studied above do not preclude the recognition of personal data as subject to property rights. On the contrary, as argued, personal data would fit the general conditions allowing individuals to exercise property rights over it.[143] Moreover, from the individual's point of view, it would seem only natural to possess his own data.[144] Even presidential candidates have recognized the importance of passing a law that grants individuals property rights over data they have generated.[145] Granting property rights over personal data would allow individuals to make decisions about their own personal data, receive compensation for use of their data, redirect the externalities of companies' use of data to the companies themselves, create incentives for companies to have more ethical treatment of data, and create spaces for data protection without the emergence of a government bureaucracy.[146] Notwithstanding this conclusion, it is necessary to give a closer look to the characteristics of property rights that govern personal data.

Property rights can be exercised over both tangible and intangible things.[147] On the one hand, intangible property rights govern objects that do not physically exist but can often be documented. While the document itself is not valuable, the information contained within might be.[148] Intangible objects can be presented in physical documents or electronic format.[149] On the other hand, tangible objects commonly come to mind when talking about property as a category of rights over things with physical properties

139. Tatum Bros. Real Est. & Inv. Co. v. Watson, 109 So. 623, 626 (Fla. 1926).

140. United States v. Craft, 535 U.S. 274, 278 (2002).

141. *See* Hildebrand v. S. Bell Tel. & Tel. Co., 14 S.E.2d 252, 256 (N.C. 1941).

142. Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1130–31 (2000).

143. *See supra* Subpart III.A.1.

144. Samuelson, *supra* note 142, at 1130.

145. *Data as a Property Right*, YANG2020, https://www.yang2020.com/policies/data-property-right/ (last visited Apr. 28, 2021).

146. *See* Samuelson, *supra* note 142, at 1132–36.

147. Adams v. Great Am. Lloyd's Ins. Co., 891 S.W.2d 769, 772 (Tex. App. 1995).

148. *Id.*

149. *See* Thyroff v. Nationwide Mut. Ins. Co., 864 N.E.2d 1272, 1275–76 (N.Y. 2007).

that can be held and touched.[150] Given its lack of physical form, data would be an intangible object that could be subject to property rights,[151] contained in either documents or electronic media.

Personal data is also a special kind of property in other respects. As in the case of intellectual property, personal data is a nonrivalrous asset in the sense that by using it, you do not exhaust its availability to others.[152] Moreover, there are certain specific rights composing the bundle of sticks over personal data. The data owner's rights—or the rights of a number of people—over the data include: data-integrity right (right to alter or destroy his data), data-use right (right to use the data for the owner's internal purposes), data-disclosure right (right to disclose or not his data), data-"copy" right (right to reproduce his data), and data-access-control right (right to regulate access to his data).[153]

Personal data should be recognized as property and those rights should be allocated to the individual to whom the data pertains.[154] The opposite conclusion would mean that individuals have no ownership of their own personas and identity.[155] Under a traditional conception based on copyright law,[156] this personal data does not belong to the subject which it describes but to the compiler who gathered the data, who would be free to exploit it.[157] However, the individual has a strong connection to the data, which describes in excruciating detail every aspect of his life—this nexus is the basis for his property claim and would be akin to the right of publicity.[158] The mere collection of personal data by companies does not create the data—its existence is tied to and extends from the individual.[159]

Although in some instances an individual is not completely capable of excluding others from knowledge of his personal data or to

---

150. *See id.* at 1277–78.

151. *But see* Jeffrey Ritter & Anna Mayer, *Regulating Data as Property: A New Construct for Moving Forward*, 16 DUKE L. & TECH. REV. 220, 255–60 (2018).

152. *See* NED SNOW, INTELLECTUAL PROPERTY, A SURVEY OF THE LAW 14 (1st ed. 2017); Raymond T. Nimmer & Patricia A. Krauthaus, *Information as Property Databases and Commercial Property*, 1 INT'L J.L. & INFO. TECH. 3, 11 (1993).

153. Nimmer & Krauthaus, *supra* note 152, at 10.

154. *See* Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1, 76 (1996).

155. *Id.* at 68.

156. "A 'compilation' is a work formed by the collection and assembling of preexisting materials or of data that are *selected, coordinated, or arranged in such a way that the resulting work as a whole constitutes an original work of authorship*." 17 U.S.C. § 101 (emphasis added); *see also* Hemnes, *supra* note 127, at 18.

157. *See* Hemnes, *supra* note 127, at 18.

158. *See* Bergelson, *supra* note 127, at 419; Nimmer & Krauthaus, *supra* note 152, at 8, 30.

159. Bergelson, *supra* note 127, at 419.

exercise the full scope of the bundle of sticks,[160] one must remember that the bundle of sticks does not necessarily remain in the dominion of the same individual at all times.[161] One illustration of this principle is the case of a building's owner who while holding the building's title also leases it to tenants who can occupy and exclude others from the building.[162]

The law is an adaptable entity that responds to the demands of the ever-advancing human societies—*rights evolve*.[163] In a very influential law review article coauthored by Samuel Warren and Justice Louis Brandeis, they argue that concepts of contract and trust were insufficient in the 1890s to prevent the perpetration of wrongs against an individual's privacy through *modern devices* such as cameras.[164] They argue that the law should create a wider protection for individuals in the form of the right of privacy, which for them was property related.[165] Based on this conception of the nature of the law and the pressures technology imposes upon it, a protection based merely on the right of privacy is insufficient and protection for the individual's property rights over his own digital identity is essential.

2. Normative Theories Supporting Individual Ownership of Personal Data

There are several competing interests seeking to take property rights over personal data for themselves.[166] The government, the public in general, companies, and individuals collide with each other to obtain property rights over personal data.[167] Nonetheless, the individual's rights are superior to all others given the private nature of the data—the individual should control the use of such data by others.[168]

There are at least four perspectives that explain why the individual's property claim to his personal data is superior: the labor theory, the utilitarian theory, the personality theory, and the blackmail argument.[169] Under the labor theory, a basic principle is that every person has ownership over himself, together with his personal data, as part of all of the things that make that person who

160. *See* Hemnes, *supra* note 127, at 19, 25–26.
161. *See* Reed v. Toyota Motor Credit Corp., 459 P.3d 253, 258 (Or. Ct. App. 2020).
162. *Id.*
163. *See* Samuel D. Warren & Louis D. Brandeis, *Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).
164. *Id.* at 211.
165. *Id.* at 211, 213.
166. Mell, *supra* note 154, at 68.
167. *See id.*
168. *See id.*
169. Bergelson, *supra* note 127, at 419–36.

he is.[170] Moreover, individuals can gain ownership through labor, provided that the good to be possessed is not already someone else's property.[171] Thus, individuals would have an inherent property right over their personal data, and collectors of data could not make the data theirs because it is already owned by the individual.[172]

Utilitarianism favors the maximization of human satisfaction, often seen as economic maximization.[173] Poor protections of property rights in personal data force individuals to spend time and money to protect themselves from the unauthorized use of their data.[174] These and other externalities produced by a company's wasteful use of personal data are shifted to individuals and society.[175] Furthermore, individual privacy is a value that should prevail in the distribution of property rights even over economic efficiency.[176] These inefficient results are contrary to the utilitarian theory under which individual rights over their personal data prevail.[177]

Under the personality theory, control over property allows the pursuit of self–development.[178] This theory considers the link a person has with an object, distinguishing between personal property—irreplaceable and subject to stronger legal protections because it aids an individual's "sense of continuity of self over time"—and fungible property—subject to weaker protections and owned for instrumental purposes—to decide between competing interests.[179] The characteristics of personal data would render it necessary for an individual's "sense of continuity of self over time" and thus an individual's claim over his personal data would prevail over a company's.[180]

Finally, the blackmail argument introduces a hypothetical question: Why should it be a crime when a blackmailer asks his victim for the payment of money in exchange for transmitting certain data—unrelated to other criminal acts—when selling the same data to a third party would be perfectly legal?[181] There are some theories that intend to explain this paradox, but at the end, their bases are moral, not legal.[182] A possible answer is that the blackmailer's rights to the data are subordinate to those of his victim—the data's true owner—

170. *Id.* at 420.
171. *Id.*
172. *Id.* at 421.
173. *Id.*
174. *Id.* at 422–23.
175. *Id.* at 424.
176. *Id.* at 427.
177. *Id.* at 425–29.
178. *Id.* at 430.
179. *Id.* at 430–31.
180. *Id.* at 431–32.
181. *Id.* at 433–35.
182. *Id.* at 433–34.

but not to those of a third party.[183] Intending to sell the data to its true owner would be theft.[184] This argument recognizes that personal data is subject to property rights, and it belongs to the individual which it describes.[185]

Accepting that personal data belongs to each individual does not mean that their rights over their data are absolute or exclusive.[186] Vera Bergelson proposes a few limitations on an individual's rights over personal data so that other interested parties, like the government, the public, and companies, can access it.[187] The first limitation that she proposes is one of duration, granting each individual a life estate over their own personal data so that privacy concerns die with the individual.[188] Second, data collectors would receive a nonexclusive and inalienable automatic license for their own internal use.[189] Third, the government and the public would also receive a nonexclusive automatic license for noncommercial purposes.[190]

Individuals should be able to exercise property rights over their personal data: they should own the data that they generate and that identifies them, they should decide how to use it, they should profit from it (if at all), and they should control the conditions surrounding the use of that data by those with whom they share it. When a company collects an individual's personal data, that company is also likely to profit from the data it has gathered.[191] The company can assign a variety of uses to the data it collected from consumers: it can reduce search costs for products via personalized and collaborative filtering of offerings, lower transaction costs for itself and consumers, conduct risk analyses on customers, increase advertising returns through better targeting of advertisements, enable the use of personal data as a user-generated content product, or transact directly with the data.[192] But what limits should contain a company's control over personal data?

B. Bailment as the Source of Plaintiff's Injury in a Data Breach Case

Starting from the point that personal data is subject to property rights vested in the individual that generates the personal data and whom such property describes, there are grounds for establishing an

183. *Id.* at 435–36.
184. *Id.*
185. *See id.* at 436.
186. *Id.*
187. *Id.* at 436–42.
188. *Id.* at 438–40.
189. *Id.* at 440.
190. *Id.* at 441–42.
191. *See* Samuelson, *supra* note 142, at 1126–27.
192. *See* Spiekermann et al., *supra* note 1, at 161.

injury traceable to the collector company in the case of a data breach. Additionally, one must remember that the mere transmission of personal data to a company does not mean that an individual has relinquished his property rights over his personal data.[193]

The ground for fulfilling Article III's requirement of an injury to the plaintiff is a breach of bailment. Although plaintiffs have already presented the idea of a bailment in personal data as the foundation of standing in data breach cases before courts, these courts have either bypassed the argument or they have limited their understanding of bailments to such a narrow view that rendered bailments obsolete.[194] Courts have primarily dismissed bailment claims in data breach cases on the following grounds: lack of agreement between the parties about the disposition of the personal data after fulfillment of the bailment's purpose, lack of intention or participation on the part of the defendant company in the perpetration of the data breach, and lack of belief in the plaintiff's assertion that he holds property rights over his personal data and that there was a delivery of that property to the defendant.[195]

1. Judicial Treatment of the Bailment Theory

Richardson v. DSW, Inc.[196] is an example of a court rejecting a bailment claim because of a narrow understanding of the doctrine, despite summarizing the argument.[197] After the theft of credit card information held by the defendant in this case, the plaintiff presented bailment as one of her claims.[198] The court was skeptical of bailments in intangible property because it asserted that such property can be subject to a bailment "in certain circumstances," with no basis for that limitation.[199] The dismissal stemmed from the lack of agreement between the parties as to the disposition of the property once the purpose of the alleged bailment was fulfilled.[200]

193. *See* Nimmer & Krauthaus, *supra* note 152, at 32.

194. *See* R.H. Helmholz, *Bailment Theories and the Liability of Bailees: The Elusive Uniform Standard of Reasonable Care*, 41 U. KAN. L. REV. 97, 97 (1992); Todd Ommen, *Bailment Claims: A Cause of Action in Data Breach Cases*, WEITZ & LUXENBERG (Apr. 14, 2015), https://www.weitzlux.com/blog/2015/04/14/bailment-claims-cause-action-data-breach-cases/.

195. *See In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1177 (D. Minn. 2014); *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942, 974 (S.D. Cal. 2012); Richardson v. DSW, Inc., No. 05 C 4599, 2005 WL 2978755, at *4 (N.D. Ill. Nov. 3, 2005).

196. No. 05 C 4599, 2005 WL 2978755 (N.D. Ill. Nov. 3, 2005).

197. *See id.* at *5.

198. *Id.* at *1.

199. *Id.* at *4.

200. *Id.*

In *In re Sony Gaming*,[201] the court also rejected the bailment theory for standing.[202] In that case, the plaintiffs' personal data were stolen by hackers that attacked Sony's systems.[203] The bailment theory was not thoroughly addressed in the plaintiffs' Consolidated Class Action Complaint.[204] The plaintiffs' Consolidated Class Action Complaint barely mentioned that the plaintiffs delivered and entrusted their personal data to the defendant for a specific purpose, that the defendant had a duty of care with respect to the entrusted data, and that the plaintiffs were harmed from the breach of that duty.[205] These allegations were insufficient to provide support for the proposition that plaintiffs have property rights over their personal data or to explain why there was a bailment.[206]

The court in *In re Sony Gaming* fundamentally rejected the bailment claim for three reasons.[207] First, the court dismissed the standard for bailments and instead sought intentional conduct on the part of the defendant as a prerequisite to rule in the plaintiffs' favor.[208] The court expected allegations of conversion or intentional conduct on Sony's part while also defining bailment as "the deposit of personal property with another, usually for a particular purpose."[209] Second, the court did not consider that personal data was delivered to the defendant with an expectation of return and that it was subject to property rights.[210] Finally, the court stated that the bailment claim was duplicative with respect to other claims presented by the plaintiffs.[211]

In re *Target Corp. Customer Data Security Breach Litigation*[212] is an application of the *Richardson* and In re *Sony Gaming* decisions.[213] Once again, the bailment claim was rejected based on skepticism over the capacity of plaintiffs to exercise property rights over personal data, the lack of an express agreement between the parties about the return of the data to its owners, and the court's requirement of intent to convert the data on the part of the defendant.[214]

---

201. 903 F. Supp. 2d 942 (S.D. Cal. 2012).
202. *Id.* at 974–75.
203. *Id.* at 950–52.
204. *See* Consolidated Class Action Complaint at 40, *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942, 974 (S.D. Cal. 2012) (No.: 3:11-md-02258-AJB-MDD).
205. *Id.*
206. *See In re* Sony Gaming, 903 F. Supp. 2d at 959–75.
207. *Id.*
208. *Id.* at 974.
209. *Id.*
210. *Id.*
211. *Id.*
212. 66 F. Supp. 3d 1154 (D. Minn. 2014).
213. *See id.* at 1177.
214. *See id.*

An example from the opposite side of the spectrum comes from *Galaria*.[215] In that case, the plaintiffs based their standing on an injury stemming from a bailment, among other claims.[216] In *Galaria*'s class action complaint, the plaintiffs stated that their personal data constituted their personal property and they were entitled to trust that the defendant company would protect the data in its possession.[217] The plaintiffs continued by alleging that the defendant's wrongful actions or inaction led to a breach of the data, which affected the value of the plaintiffs' personal data.[218] Therefore, the plaintiffs contended that the defendant breached its duty to safeguard and protect the plaintiffs' data by failing to maintain reasonable and effective data practices.[219]

The plaintiffs in *Galaria* were successful in their appeal and were granted standing by the Sixth Circuit.[220] However, the Sixth Circuit did not address the bailment argument and did not explain where its strength resided; thus, there is no potential for this decision to serve as the basis for this new standing doctrine.[221] In *Galaria*, the Sixth Circuit directly stated that the "allegations of a substantial risk of harm, coupled with reasonably incurred mitigation costs" were enough to satisfy the injury prong for standing—without making any reference to an injury based on a breach of bailment.[222] In other words, while the court granted standing and said it "reverse[s] the dismissal of Plaintiffs' . . . bailment" claim,[223] its decision was based on a likelihood of future harm and the costs of mitigation,[224] not on the injury suffered in the form of depreciation of the plaintiffs' personal data caused by the breach of bailment. *Galaria* is another exemplification of the circuit split in data breach cases, not a case breaking from it.

2. Overcoming the Bailment Theory's Negative Treatment

Some of the definitions of bailment explored in this Comment, while helpful, may prove insufficient. The most effective conception of a bailment is as "the rightful possession of a chattel by one who is not also the owner."[225] Definitions that prioritize elements of delivery and terms between the parties are inadequate to afford sufficient

215. 663 F. App'x 384, 384–91 (6th Cir. 2016).
216. Class Action Complaint at 1–3, Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384 (6th Cir. 2016) (No. 2:13-cv-118).
217. *Id.* at 23.
218. *Id.* at 23–24.
219. *Id.* at 24.
220. *See Galaria*, 663 F. App'x at 391.
221. *Id.* at 384–91.
222. *Id.* at 388.
223. *Id.* at 391.
224. *Id.* at 388.
225. Helmholz, *supra* note 194, at 97.

vitality to the doctrine of bailments and to explain involuntary, gratuitous, and implied bailments.[226] Thus, the core of the legal concept of bailments that applies to its different forms is *lawful possession*.[227] This definition of bailment would be broad enough to cover the relationship between a finder of lost goods and their rightful owner, who are beyond a doubt a bailee and bailor.[228] No matter how the element of lawful possession is created between the bailee and the bailor's property, a bailment arises when the bailee is accounting for the bailor's property.[229]

Courts that have explored the application of bailment claims in data breach cases have limited their understanding of this doctrine to the point of obsolescence. Such an understanding of bailments leaves out important legal concepts such as an implied-in-law bailment.[230] As stated before, the element of lawful possession while accounting for the property of another is what defines a bailment in the different forms it can arise.[231] In an implied-in-law bailment, where a person comes into possession of property and exercises control over it even if that is done for a purpose other than bailment, the law imposes over such person the duties and obligations of a bailee.[232] Another scenario where this type of bailment arises is where a person engages another to perform some service "with respect to [the bailor's] personal property, without instructions as to the property's disposition."[233]

Where a consumer provides his data to a company or where that company tracks the consumer's data, the consumer continues to hold the same property rights over the data; he does not relinquish his property rights.[234] Additionally, as explained above, it is common for the terms controlling the relationship between consumers and social media companies to specify what would happen to the data after the purpose of the relationship is fulfilled.[235] Therefore, where the facts indicate such terms exist, courts should consider those terms as indicating an agreement about how to dispose of the data. Where no terms about the disposition of the data exist, while their existence is not dispositive, it can be argued that it is implicit that the company can hold the data until its owner reclaims it.[236]

Moreover, the company is holding the data for the purpose of providing a service related to the property while it remains the

---

226. *Id.* at 98.
227. *Id.*
228. *Id.*
229. *See* Zuppa v. Hertz Corp., 268 A.2d 364, 366 (N.J. Super. Ct. 1970).
230. *See* 8A AM. JUR. 2D *Bailments* § 38 (2020).
231. *See id.*
232. *See id.*
233. *Id.*
234. Nimmer & Krauthaus, *supra* note 152, at 32.
235. *See supra* text accompanying notes 114–19.
236. 8A AM. JUR. 2D, *supra* note 230, § 38; C.J.S., *supra* note 102, § 1.

customer's property—this is a scenario where a bailment can arise.[237] This means that the company is lawfully holding the property of another while accounting for it because no rights were relinquished by the customer, and that would be enough to constitute a bailment.[238] Depending on the specifics of each case and the bailment elements present, the bailment could be based on an express contract or the bailment could be implied.[239]

Additionally, no definition of bailment presented in this Comment suggests that the bailee's intention in damaging the property is a constitutive element of a bailment.[240] A plaintiff in a data breach case is initially trying to establish that there was in fact a bailment over the data and that the personal property depreciated in order to meet the standing threshold.[241] Whether or not the defendant is liable for such depreciation would be a question for the court.[242] This Comment is only concerned with bringing plaintiffs to court because they are the proper parties to bring this claim. Even if the complaining party has to establish that the defendant is liable at the outset of the case to obtain standing, the standard of care is not one of intentionality.[243] Where both parties draw a benefit from the existence of the bailment, the bailee owes the bailor a standard of ordinary care in holding the property.[244] Here, the consumer draws the benefit of having a certain service rendered to him while the company obtains a financial gain. Thus, as both parties would benefit, the applicable standard would be ordinary care.[245]

Finally, courts are in disbelief that personal data is in fact subject to property rights and that it can be delivered as such.[246] This Comment has already presented a discussion on why personal data can be considered a form of property.[247] It can be drawn from this discussion that there is no reason, without more, to create a dividing line between traditional forms of property and personal data.[248] In fact, the court opinions studied in this Comment do not present

237. 8A AM. JUR. 2D, *supra* note 230, § 38; *see supra* text accompanying notes 114–19.

238. 8A AM. JUR. 2D, *supra* note 230, § 38.

239. *Id.*; C.J.S., *supra* note 102, § 3; 8A TEX. JUR. 3D *Bailments* § 4 (2020).

240. *See supra* Subpart II.D.

241. *See In re* Supervalu, Inc., 870 F.3d 763, 765–68 (8th Cir. 2017).

242. *See* Attias v. Carefirst, Inc., 865 F.3d 620, 625 (D.C. Cir. 2017).

243. 46 AM. JUR. PROOF OF FACTS 3D *Bailee's Liability for Damage, Loss, or Theft of Bailed Property* § 5 (2020).

244. *Id.*

245. *Id.*

246. *See In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1177 (D. Minn. 2014); *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942, 974 (S.D. Cal. 2012); Richardson v. DSW, Inc., No. 05 C 4599, 2005 WL 2978755, at *4 (N.D. Ill. Nov. 3, 2005).

247. *See supra* Subpart III.A.

248. *See supra* Subpart III.A.

concrete arguments to deny personal data the stature of property.[249] The courts' views are too traditionalist and threaten to make the law's adaptation to new technologies slower—it has to be remembered that rights evolve.[250] Future plaintiffs must take the opportunity to present stronger arguments on why their data is personal property in subsequent cases.[251]

On the other hand, delivery can be understood as the "act of transferring something . . . [by] giving or yielding possession or control of something to another."[252] A consumer that provides his personal data to a collector company yields control over it to the company—the company then exercises control over the data.[253] The company is able to sell the data, classify it in databases, use it to generate ads, etc.[254] There is no gain in drawing artificial distinctions between traditional property and personal data; it is an asset with monetary worth that can meet the law's requirements to be deemed subject to property rights.[255]

In sum, a consumer is acting as a bailor that entrusts or delivers his personal property to a bailee—in this case, a company—for the purpose of enabling the company to provide the consumer with its services.[256] They have created a bailment beyond whatever else they might have agreed to in writing or otherwise, even when a potential contract they may have reached does not mention the bailment.[257] A breach of this relationship would give rise to a right to vindicate the rights trespassed.[258] By the transfer of the customer's personal data to the company, the parties created a bailment for the mutual benefit of the parties.[259]

When the companies holding the personal data fail to meet their duty of ordinary care, the consumers would suffer a redressable injury in fact[260] because their personal property (in the form of data) has been stolen or damaged and that potentially decreases its value. Given that their personal data, as other forms of personal property, have a monetary value, the consumers' injuries are also quantifiable and specific to them.[261] The injuries the customers suffered have

249. *See* In re *Target Corp.*, 66 F. Supp. 3d at 1177; In re *Sony Gaming*, 903 F. Supp. 2d at 974; *Richardson*, 2005 WL 2978755, at *4.
250. *See* Warren & Brandeis, *supra* note 163, at 193.
251. *See supra* Subpart III.B.1.
252. *Delivery*, BLACK'S LAW DICTIONARY (9th ed. 2009).
253. Spiekermann et al., *supra* note 1, at 161.
254. *Id.*
255. *See* Mell, *supra* note 154, at 76; Spiekermann et al., *supra* note 1, at 161.
256. *See* 8A AM. JUR. 2D, *supra* note 230, § 38; C.J.S., *supra* note 102, § 1.
257. *See* 8A AM. JUR. 2D *supra* note 230, § 38; *see supra* Subpart II.D.
258. *See* 8A AM. JUR. 2D, *supra* note 230, § 204.
259. *See id.* § 38.
260. *See* C.J.S., *supra* note 102, § 55.
261. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 402 (2013).

already taken place; they are not some hypothetical or implausible future occurrence.[262]

As opposed to the positions taken by the circuit courts, the alternative presented here considers the facts as they have taken place and not the likelihood of an unlawful possessor of personal data using it in the future.[263] Although some courts are prone to finding standing under that argument because they understand the hacker's threatened use of the data as concrete enough,[264] other courts disagree and see that threat as too speculative.[265] The depreciation of a bailor's property is an injury that has already taken place.

C. Recommendations

This Subpart addresses some arguments that plaintiffs could present to make their standing claims potentially more successful. One possible improvement that can increase plaintiffs' likelihood of meeting the threshold to have standing is drafting their complaints to detail why they had a property interest in their personal data.[266] It is not enough to say that the data was indeed property; plaintiffs ought to explain why the leakage of their data causes an injury in fact.[267] In an ideal scenario, a complaining party should at least explain with detail why his personal data constitutes personal property, what injury he suffered—the depreciation in his personal data—and how that depreciation is traceable to the defendant. An alternative to attain this goal is to be explicit about the monetary value behind personal data, highlighting the economic gain others—including collector companies and hackers—draw from plaintiffs' personal data even though it does not constitute their property.[268]

---

262. *See id.*

263. *See In re* Zappos.com, Inc., 888 F.3d 1020, 1023, 1030 (9th Cir. 2018); Attias v. Carefirst, Inc., 865 F.3d 620, 622, 626–67, 670 (D.C. Cir. 2017); Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 89–91 (2d Cir. 2017); Beck v. McDonald, 848 F.3d 262, 266–67, 274–75 (4th Cir. 2017); *In re* Supervalu, Inc., 870 F.3d 763, 766–67, 770 (8th Cir. 2017); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 384–88 (6th Cir. 2016); Remijas v. Neiman Marcus Grp., 794 F.3d 688, 690–91, 694–95, 697 (7th Cir. 2015).

264. *See* In re *Zappos.com, Inc.*, 888 F.3d at 1028; *Attias*, 865 F.3d at 630; *Galaria*, 663 F. App'x at 388; *Remijas*, 794 F.3d at 693.

265. *See* In re *Supervalu, Inc.*, 870 F.3d at 770–72; *Whalen*, 689 F. App'x at 91; *Beck*, 848 F.3d at 274–75, 278.

266. *See In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1177 (D. Minn. 2014); *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942, 974 (S.D. Cal. 2012); Richardson v. DSW, Inc., No. 05 C 4599, 2005 WL 2978755, at *4 (N.D. Ill. Nov. 3, 2003).

267. *See* In re *Target Corp.*, 66 F. Supp. 3d at 1177; In re *Sony Gaming*, 903 F. Supp. 2d at 974; *Richardson*, 2005 WL 2978755, at *4.

268. *See* In re *Supervalu, Inc.*, 870 F.3d at 772–74; In re *Target Corp.*, 66 F. Supp. 3d at 1177; In re *Sony Gaming*, 903 F. Supp. 2d at 974; *Richardson*, 2005 WL 2978755, at *4; Spiekermann et al., *supra* note 1, at 161.

Furthermore, plaintiffs can benefit from providing detailed accounts of how they relinquished control of their personal data to the collector company.[269] This could include a description of the data submitted through forms, any permissions plaintiffs gave to the collector company to track additional data, and any restraints preventing plaintiffs from freely accessing the files companies held about them.

Plaintiffs can also draft arguments about the creation of the bailment relationship.[270] The cases studied here, while differing in the degree of detail about the alleged bailments between the consumers and the companies, did not address the kind of bailment that applied in each instance.[271] The courts had too much room to present arguments about bailments in general that were not directly relevant in those cases.[272] Moreover, in cases where consumers do have some bargaining power, it would be in their best interest to negotiate the inclusion of terms that expressly recognize the existence of a bailment between the parties.

After providing a strong basis for the existence of the bailment relationship, plaintiffs could also give more details about the applicable standard of care for the specific form of bailment they created.[273] This discussion can be accompanied by a few words on the pleading requirements at the stage standing is decided as a way to remind the court that plaintiffs do not have to prove every element of their cause of action to get standing.[274]

The central issue of this Comment is not whether defendants should be liable for breaches: it is only whether courts should hear plaintiffs' claims. The current state of the law provides inconsistent treatment to plaintiffs that merely attempt to present their claims. Once the courtroom doors are equally open for data breach plaintiffs in similar circumstances, a defendant's liability will depend on the specific facts of each case and each jurisdiction's applicable law.

Although these recommendations do not ensure that plaintiffs will be granted standing and have the opportunity to present the full scope of their cases before a court, the recommendations address some of the issues that courts have paid attention to in issuing decisions

---

269. *See* In re *Sony Gaming*, 903 F. Supp. 2d at 974.

270. *See id.*

271. *See* In re *Target Corp.*, 66 F. Supp. 3d at 1177; In re *Sony Gaming*, 903 F. Supp. 2d at 974–75; *Richardson*, 2005 WL 2978755, at *4.

272. *See* In re *Target Corp.*, 66 F. Supp. 3d at 1177; In re *Sony Gaming*, 903 F. Supp. 2d at 974–75; *Richardson*, 2005 WL 2978755, at *4.

273. *See* AM. JUR. PROOF OF FACTS 3D, *supra* note 243, § 5 (explaining the applicable standards of care in bailments).

274. *See* Attias v. Carefirst, Inc., 865 F.3d 620, 625 (D.C. Cir. 2017).

that denied standing to plaintiffs that presented a theory for their claims based on bailments.[275]

IV. CONCLUSION

Standing in data breach cases can be a convoluted area of the law.[276] While this Comment does not come near to finding a solution that accounts for all of the complex interests involved in data breach cases, it presents an alternative to allow plaintiffs to have a voice and stand up in court and present their cases. Going back to the standards for finding an injury under *Clapper*, asserting a breach of the bailment relationship in a data breach case does not rely on a too attenuated chain of possibilities.[277] The harm to plaintiffs' property is an injury that has already taken place; it is not a threatened injury that needs to qualify as either a certainly impending injury or one that creates a substantial risk of harm.[278] This way, the alternative presented in this Comment breaks free from the present circuit split to argue that the basis for standing can be found in the facts that have already taken place.

Raquel González-Padrón[*]

275. *See* In re *Target Corp.*, 66 F. Supp. 3d at 1177; In re *Sony Gaming*, 903 F. Supp. 2d at 974–75; *Richardson*, 2005 WL 2978755, at *4.

276. *See, e.g.*, *In re* Zappos.com, Inc., 888 F.3d 1020 (9th Cir. 2018); *In re* Supervalu, Inc., 870 F.3d 763 (8th Cir. 2017); *Attias*, 865 F.3d 620; Whalen v. Michaels Stores, Inc., 689 F. App'x 89 (2d Cir. 2017); Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384 (6th Cir. 2016); Remijas v. Neiman Marcus Grp., 794 F.3d 688 (7th Cir. 2015).

277. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 410–14 (2013).

278. *See id.* at 409–10, 414 n.5.

* J.D. Candidate 2021, Wake Forest University School of Law. Licenciada en Ciencia Política, *summa cum laude*, 2016, Universidad del Zulia. I would like to thank Neida Padrón and Eddy Mogollón for their support and for helping me get from Cabimas to Wake Forest. Thank you to Wyrick Robbins' Privacy & Data Security team for suggesting standing in data breach cases as a topic. Special thanks to Professor Andrew Verstein for his advice in developing and refining this Comment. Finally, thank you to all the *Wake Forest Law Review* members for their invaluable work in improving this Comment.