Washington and Lee Law Review

Volume 76 | Issue 2 Article 9

6-19-2019

Text Messages Are Property: Why You Don't Own Your Text Messages, but It'd Be a Lot Cooler if You Did

Spence M. Howden
Washington and Lee University School of Law, howden.s@law.wlu.edu

Text Messages Are Property: Why You Don't Own Your Text Messages, but It'd Be a Lot Cooler if You Did

Spence Howden*

Table of Contents

* J.D. Candidate May 2019, Washington and Lee University School of Law. I am grateful to Professor Fairfield for contributing his insight and expertise on this topic. Thanks to the editorial board, Chris, Matt, James, and my mom for their guidance and edits. This Note would not have been possible without the unending support of my family and my wonderful girlfriend, Elizabeth. Finally, I thank Mr. Cruz, for teaching me in ninth-grade English that writing was cool.

I. Introduction

Consider this scenario: an automatic Apple iPhone update deletes all of Jane's text messages. Jane's iPhone is wiped clean, and there is nothing she can do to get her text messages back. Apple will quickly send out a carefully crafted apology, which subtly points out that Jane accepted the risk of this happening due to some obscure provision in their terms of service she never read. This rings hollow, though, because Jane still feels like she lost something of value, something she owned. Even though they were just words on a screen, Jane's text messages were a little bit more than that to her—they felt like a part of who Jane is and who she was.

These text messages were more than just data and binary code. They contained Jane's personal information and correspondence with friends and family over the years. To Jane, those virtual text messages felt like her property; she had created the outgoing messages and received the incoming messages. Even if she clicked away her right to pursue contractual remedies by accepting Apple's terms of service, is there anything Jane can do?

As of today, the answer is a resounding "no."[1] Jane would be surprised to learn that she cannot successfully sue Apple for

1. *Infra* Part IV.A.

deleting her text messages because her text messages are not considered personal property. Because text messages are not a "property," she would not be able to successfully bring a conversion or trespass claim, despite the elements of both claims being met.[2] Instead, Jane would be limited to a breach of contract claim, limiting her chances of redress for Apple's deletion of something that feels like her personal property.[3]

Therein lies the problem: courts do not treat text messages as intangible personal property. Authors and recipients of text messages have limited recourse against cell phone manufacturers or service providers when they "accidentally" delete their users' text messages. Instead, courts consider text messages to be the product of the contract for services between the cell phone user and the cell phone provider. Put another way, because text messages would not exist but-for a cellular service contract, they are not considered property. Under this "contractually created right" theory, text message users can bring an action for a breach of contract when their text messages are improperly deleted, but that's about it. Should courts treat text messages as a purely contractual right, or should text messages constitute intangible personal property capable of being owned?

This Note argues that text messages are intangible personal property. This leads to two practical outcomes. First, text message "owners" can successfully sue using property-based causes of action (e.g., trespass to chattels and conversion) when their ownership rights over their text messages are disturbed by the service provider or cell phone manufacturer. Second, the property rights inherent in text messages will limit the government's power under the third-party doctrine.

This Note proceeds as follows: Part II offers a brief overview of what text messages are and what they are not. Part III covers the history of intangible personal property law and reviews the evolution of "cybertrespass" claims. Part IV explores the judiciary and the Fourth Amendment's failure to protect text messages. Finally, Part V evaluates whether text messages constitute property and the practical implications of this finding.

---

2. *Infra* Part V.A.2.
3. *Infra* Part IV.A.1.

II. Text Messages: An Overview

Text messaging (or texting) is a text-based form of communication between cell phone users.[4] Text messages, as an alternative to e-mails and phone calls,[5] are the predominant form of communication in society.[6] The broad term "text messages" encompasses text-only messages sent via Short Messages Service (SMS), picture, video and sound messages (multimedia messages or MMS), and messages sent through third-party messenger applications such as iMessage.[7] SMS and MMS messages are transmitted from the sender's cell phone to an SMS tower, which then sends the messages to the cell phone service provider's tower, which then dispatches the text message to the recipient's cell phone.[8] Messenger applications use cellular provider data networks to send text and multimedia messages between mobile phone users who possess the same messenger application downloaded on their phones.[9]

Cell phones are so ingrained in American culture that "[n]o one ever leaves the house these days without three things: their keys, wallet and mobile [device]. It is, in short, an essential lifestyle accessory."[10] Ninety-five percent of American adults own

---

4. *See* Moore v. Apple, Inc., 309 F.R.D. 532, 536 (N.D. Cal. 2015) (defining text messaging).

5. *See In re* Text Messaging Antitrust Litig., 782 F.3d 867, 869 (7th Cir. 2015) ("Text messaging is thus an alternative both to email and to telephone calls.").

6. *See* State v. Hinton, 280 P.3d 476, 490 (Wash. Ct. App. 2012) (discussing the societal shift in Americans' private communications methods from phone calls and letters to text messaging).

7. *See Moore*, 309 F.R.D. at 536 ("Texting originally only referred to messages sent using the Short Messages Service ('SMS'), but now also encompasses messages containing media such as pictures, videos, and sounds ('MMS').").

8. *See id.* (explaining the route SMS and MMS messages take from the sender's mobile phone to the receiver's mobile phone).

9. *See id.* (distinguishing iMessage and other messenger services from SMS and MMS messages).

10. Anthony Patterson, *Digital Youth, Mobile Phones and Text Messaging: Assessing the Profound Impact of a Technological Afterthought*, *in* THE ROUTLEDGE COMPANION TO DIGITAL CONSUMPTION 83 (Russell W. Belk & Rosa Llamas eds., 2013).

a cell phone.[11] Nearly three-quarters of American adults who own cell phones send and receive text messages.[12] Text messaging users, on average, send or receive more than forty-one messages daily, while cell phone owners make or receive an average of ten phone calls daily.[13] In short, most Americans own cell phones, and Americans use their cell phones to text message more often than they do to make phone calls or send e-mails.

Although the majority of this Note concerns what text messages are, it is helpful to narrow the issue's scope and briefly explain what text messages are not. Text messages are not physical or tangible objects.[14] Text messages are not copyrightable and thus not protected by intellectual property law.[15] And text messages are not e-mails.[16]

A. Text Messages Are Not Physical Property nor Are They Protected by Copyright

At the outset, it is important to distinguish the intangible data and text messages contained within the cell phone from the physical, tangible cell phone object. For example, during an arrest, the police can search the exterior of a cell phone, but they are barred from searching the data housed in the phone.[17] Internal cell phone data, contained within a "smart" object, carries greater constitutional protections than objects held within "simple"

---

11. *See Mobile Fact Sheet*, PEW RES. CTR. (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/mobile/ (last visited Mar. 19, 2019) (detailing trends in mobile phone ownership over time) (on file with the Washington and Lee Law Review).

12. *See* Aaron Smith, *Americans and Text Messaging*, PEW RES. CTR. (Sept. 19, 2011), http://www.pewinternet.org/2011/09/19/americans-and-text-messaging/ (last visited Mar. 19, 2019) (describing trends in text message usage among Americans over time) (on file with the Washington and Lee Law Review).

13. *Id.*

14. *Infra* Part II.A.

15. *Infra* Part II.A.

16. *Infra* Part II.B.

17. *See* Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CAL. L. REV. 805, 833–34 (2016) ("The physical object (the phone) could be searched to ensure, for example, that a razor blade was not hidden inside, but the digital content could not be searched without a warrant.").

containers.[18] Additionally, although a cell phone owner owns the physical device itself, the owner does not own the software contained within, as cell phone providers license (rather than sell) the software to the cell phone owner for their use.[19]

Just as there is a distinction between the ownership of the physical phone and the data and software within, there is also a distinction between owning the copyright to the contents of a text message and owning a copy of the text message itself. This is the "copy/copyright" distinction. In relevant part, the Copyright Act[20] states that "[o]wnership of a copyright, or of any of the exclusive rights under a copyright, is distinct from ownership of any material object in which the work is embodied."[21] The copy/copyright distinction is crucial when establishing ownership rights held in an intangible property such as a text message,[22] and understanding the copy/copyright distinction is necessary for this reason: intellectual property law governs copyrights, but property law governs ownership rights in the underlying material "copy" or object itself.[23]

The ownership of a copyright to the content of a given text message hinges on the length of the text message.[24] If a text message is short, as most text messages tend to be, the author does

---

18. *See id.* at 834 ("[T]he Court implicitly creates a distinction between simple objects and smart objects (with data inside), with the latter being granted additional protection.").

19. *See* Aaron Perzanowski & Jason Schultz, *Reconciling Intellectual and Personal Property*, 90 NOTRE DAME L. REV. 1211, 1253–60 (2015) (explaining that the majority of courts classify software transactions as licenses instead of sales).

20. 17 U.S.C. § 202 (2012).

21. *See id.* (distinguishing ownership of a copyright from ownership of an object).

22. *See* Perzanowski & Schultz, *supra* note 19, at 1216 ("The exhaustion principle, though historically associated with a clear distinction between copy and copyright, is in fact the primary tool in copyright law for mediating the somewhat indistinct line separating the copy and the work.").

23. *See* 17 U.S.C. § 202 (distinguishing ownership of a copyright from ownership of an object).

24. *See* Edina Harbinja, *Legal Nature of Emails: A Comparative Perspective*, 14 DUKE L. & TECH. REV. 227, 235–36 (2016) ("To conclude, despite long emails meeting the requirement of originality and fixation, there would be a regulatory vacuum for a significant number of short emails.").

not hold the copyright to the content of that message.[25] However, the author likely has copyright protection over the content of the text message if the text message is lengthy and more complex, an "original work of authorship," and is "electronically fixated."[26] Even though copyright law might protect some text messages, copyright law alone is not adequate to protect all text messages, and does not protect the text message recipient.[27] Thus, because copyright law does not effectively protect text message authors and recipients, property law should fill the needed gap and give text message owners the rights against intrusive cellular service providers to which they are entitled.

B. Are Text Messages Distinguishable from E-Mails?

The distinction between text messages and e-mails is subtle, but there are some fundamental differences between the two.[28] In particular, text messages are distinguishable from e-mails both in how society uses text messages to communicate and in how text messages mechanically operate.[29]

While both the judiciary and the legal academy have addressed the status of e-mails as "property," the same question regarding text messages has gone unanswered.[30] Most

---

25. U.S. COPYRIGHT OFFICE, MULTIPLE WORKS 2 (2019), https://www.copyright.gov/circs/circ34.pdf.

26. *See* Harbinja, *supra* note 24, at 235 (explaining that longer e-mails meet the originality and fixation copyright requirements).

27. *Id.*

28. *See* Joseph C. Vitale, Note, *Text Me, Maybe?:* State v. Hinton *and the Possibility of Fourth Amendment Protections Over Sent Text Messages Stored in Another's Cell Phone*, 58 ST. LOUIS U. L.J. 1109, 1141 (2014) (arguing that text messages differ from e-mails because of the different ways society utilizes the technologies).

29. *See id.* at 1140–41 (distinguishing text messages from e-mails); Katharine M. O'Connor, Note, *:o OMG They Searched My Txts: Unraveling the Search and Seizure of Text Messages*, 2010 U. ILL. L. REV. 685, 686 ("[T]ext messages, unlike letters or e-mails, have in the past only been generally accessible through a mobile device.").

30. *See, e.g.*, Porters Bldg. Ctrs., Inc. v. Sprint Lumber, No. 16-06055-CV-SJ-ODS, 2017 WL 4413288, at *11 (W.D. Mo. Oct. 2, 2017) (determining that e-mails constitute intangible personal property); *infra* note 31 (collecting legal scholarship that addresses the question of whether e-mail is property).

commentators who have addressed the issue with regard to e-mails advocate for the treatment of e-mails as property.[31]

Courts routinely consider whether e-mails constitute descendible intangible personal property in the probate context (and often find that they are property in probate cases), but courts do not consider whether text messages constitute property with the same regularity.[32] And the recent surge of federal district courts concluding that e-mails constitute intangible property indicates that the first "text messages are property" case could be right around the corner.[33] The ever-increasing popularity of text messages likely signals that courts will have to tackle the issue of whether text messages constitute property in the coming years.[34] What someone might have sent via e-mail ten years ago is sent via text message today, and thus issues regarding text message ownership will become more and more common.[35]

---

31. *See, e.g.*, Jennifer Arner, Comment, *Looking Forward by Looking Backward:* United States v. Jones *Predicts Fourth Amendment Property Rights Protections in E-mail*, 24 GEO. MASON U. C.R.L.J. 349, 379 (Summer 2014) ("[I]f the Court is willing to recognize true property rights in particular forms of electronic communication, the property-centered approach relied on in *Jones* will afford bright-line protections for these intangible interests."); Justin Atwater, *Who Owns E-Mail? Do You Have the Right to Decide the Disposition of Your Private Digital Life?*, 2006 UTAH L. REV. 397, 418 ("Although e-mail shares qualities with both tangible and intangible property, the differences create enough of a distinction that the laws of property cannot effectively deal with who owns e-mail."); Jonathan J. Darrow & Gerald R. Ferrera, *Who Owns a Decedent's Emails: Inheritable Probate Assets or Property of the Network?*, 10 N.Y.U. J. LEGIS. & PUB. POL'Y 281, 319 (2007) ("The ownership and intellectual property interests authors have in their electronically stored e-mail accounts are no less legitimate than are such interests in messages created with paper and pen."). *But see* Harbinja, *supra* note 24, at 254 ("Based upon current copyright and property law, and upon the western theories of property, the legal nature of email appears clear. Email content is not the property of its users.").

32. *See, e.g.*, Atwater, *supra* note 31, at 400–02 (discussing how a probate court forced Yahoo! to hand over a deceased marine's e-mails to his parents).

33. *Infra* notes 118–126 and accompanying text.

34. *See* Moore v. Apple Inc., 309 F.R.D. 532, 536 (N.D. Cal. 2015) (explaining how text messaging has become "the most widely used mobile data service").

35. *See* Lydia Dishman, *Texting Is The New Email—Does Your Company Do It Right?*, FAST COMPANY (May 30, 2013), https://www.fastcompany.com/3010237/texting-is-the-new-email-does-your-company-do-it-right (last visited Mar. 22, 2019) ("[T]exting—to the tune of 9.8 trillion sent in 2012—is becoming the new medium through which companies

III. The History of Intangible Property Law and Cybertrespass

Intangible personal property, as its name suggests, is a personal property or a "chattel" that cannot be physically touched.[36] Text messages are a form of "digital" property, which is arguably a type of intangible personal property.[37] Courts are split on whether disrupting possession of someone's intangible property is equivalent to disrupting possession of physical property, or, instead, breaching a contractually created right.[38] If a court treats a dispute over theft of intangible property as a dispute over personal property, the aggrieved party can pursue a conversion or trespass to chattels tort claim for the disruption of their intangible property rights.[39] However, if a court treats the same dispute as a potential breach of a contractually created right, the aggrieved party cannot bring a tort law cause of action and is limited to contractual remedies.[40]

The principal cases involving disputes over the property status of intangible personal property concerned perhaps the earliest widely available digital asset: internet domain names.[41] These cases determined whether a domain name was a type of property, and if it was, whether the aggrieved party could pursue a traditional property-based claim against the domain name

---

communicate.") (on file with the Washington and Lee Law Review).

36. *See Intangible Personal Property*, INVESTOPEDIA, https://www.investopedia.com/terms/i/intangible-personal-property.asp (last updated Feb. 12, 2018) (last visited Mar. 19, 2019) ("Intangible personal property is something of individual value that cannot be touched or held.") (on file with the Washington and Lee Law Review).

37. *Id.*

38. *See* Kremen v. Cohen, 337 F.3d 1024, 1029–36 (9th Cir. 2003) (finding that the taking of an intangible property provided the basis for a property law conversion claim). *But see* Network Sols., Inc. v. Umbro Int'l, Inc., 529 S.E.2d 80, 85–88 (Va. 2000) (finding that the taking of an intangible property disrupted a contractual, and not a property, right).

39. *See Kremen*, 337 F.3d at 1029–36 (determining that the defendant's giving away of the plaintiff's intangible property without his consent "supported a claim for conversion").

40. *See Umbro*, 529 S.E.2d at 85–88 (explaining that a domain name, although an intangible property, is the product of a service contract that does not exist separate from the service that created it and is therefore a contractually created right).

41. *Infra* Part III.A–B.

registrar.[42] To be sure, text messages are not domain names, but both text messages and domain names arguably constitute forms of intangible personal property.[43] Accordingly, the courts' reasoning in the domain name cases applies to situations involving other intangible personal properties, such as text messages.[44]

This Part, in subparts A and B, proceeds by analyzing the two leading cases for and against the theory that digital property constitutes intangible personal property. Then, subpart C contrasts these two cases and explores what drove the courts to come out on opposite sides of the issue. Finally, subpart D tracks the evolution of property law tort remedies as applied to digital property and examines recent federal court cases determining that e-mails constitute property.

A. The Intangible Personal Property Theory: Digital Assets Can Be Owned

Enter *Kremen v. Cohen*.[45] *Kremen* involved a California plaintiff, Gary Kremen, who sought conversion damages from a defendant who stole Kremen's internet domain name.[46] Kremen bought the domain name "sex.com" through a domain name registrar.[47] Shortly thereafter, a con man named Stephen Cohen duped the domain name registrar into transferring possession of Kremen's sex.com domain name to Cohen's account.[48] Kremen then sued Cohen and the domain name registrar, claiming that the tort of conversion applied to Cohen's stealing Kremen's sex.com domain name.[49]

---

42. *Infra* Part III.A–B.

43. *Infra* Part V.A.

44. *Infra* Part V.A.

45. 337 F.3d 1024 (9th Cir. 2003).

46. *See id.* at 1026 ("We decide whether Network Solutions may be liable for giving away a registrant's domain name on the basis of a forged letter.").

47. *Id.*

48. *Id.* at 1027.

49. *See id.* at 1028 ("His third theory is that he has a property right in the domain name sex.com, and Network Solutions committed the tort of conversion by giving it away to Cohen.").

Before Kremen could prove the tort of conversion, he first had to prove that the domain name Cohen took constituted a piece of property.[50] The Ninth Circuit defines property as a "broad concept that includes every intangible benefit and prerogative susceptible of possession or disposition."[51] Under the court's three-part test, a digital asset constitutes personal property if: (1) there is "an interest capable of precise definition"; (2) it is "capable of exclusive possession or control"; and (3) there is a "legitimate claim to exclusivity."[52]

The Ninth Circuit found that domain names satisfied each criterion required under the three-part property test.[53] First, the court explained that domain names are capable of precise definition because the person who registers the domain name chooses exactly where on the internet those who type that particular domain name are sent.[54] Second, the court noted that domain names are capable of exclusive possession or control because the registrant alone decides on what the domain name will be.[55] Finally, the court reasoned that there is a legitimate claim to exclusivity with regard to domain names, because registering a domain name is a way of communicating sole ownership of the internet domain to others, ensuring registrants gain a benefit on their time and money spent developing their websites, and encouraging investment in domain names and the internet overall.[56]

---

50. *See id.* 1029–30 (explaining that Kremen must first establish that he had a property right in the domain name before he can make a conversion tort claim).

51. *Id.* at 1030.

52. *Id.*

53. *See id.* (finding that "Kremen therefore had an intangible property right in his domain name").

54. *See id.* ("Like a share of corporate stock or a plot of land, a domain name is a well-defined interest.").

55. *See id.* ("Ownership is exclusive in that the registrant alone makes that decision.").

56. *See id.* at 1030

> Registrants have a legitimate claim to exclusivity. Registering a domain name is like staking a claim to a plot of land at the title office. It informs others that the domain name is the registrant's and no one else's. Many registrants also invest substantial time and money to develop and promote websites that depend on their domain names.

After determining that Kremen owned property rights to his domain name, the court analyzed whether the tort of conversion applied to disputes regarding intangible property.[57] Historically, intangible property conversion claims required that a document exist where the intangible rights are merged into the physical document.[58] This means that there is a physical document that represents and is equivalent to the intangible obligation (e.g., a stock certificate representing ownership of a share of stock).[59] However, the court explained that courts in California had rejected the strict merger requirement. But, even if the merger requirement applied, it was minimal and required only some relationship with a tangible object.[60] The court reasoned that Kremen's sex.com domain name digital file must be stored within a physical computer associated with the domain name provider somewhere, and found that this connection was sufficient to satisfy conversion's merger requirement.[61]

This finding, coupled with the court's determination that Kremen had a property right in his domain name, led the court to conclude that Kremen brought a viable conversion claim.[62] In closing, the court justified its conclusion by noting that "the

---

57. *See id.* at 1029 ("To establish that tort, a plaintiff must show 'ownership or right to possession of property, wrongful disposition of the property right and damages.'" (quoting G.S. Rasmussen & Assocs., Inc. v. Kalitta Flying Serv., Inc., 958 F.2d 896, 906 (9th Cir. 1992))).

58. *See id.* at 1031

> An intangible is "merged" in a document when, "by the appropriate rule of law, the right to the immediate possession of a chattel and the power to acquire such possession is represented by [the] document," or when "an intangible obligation [is] represented by [the] document, which is regarded as equivalent to the obligation."

(quoting RESTATEMENT (SECOND) OF TORTS § 242 cmt. a (AM. LAW INST. 1965)).

59. *Id.*

60. *See id.* at 1033 ("Assuming *arguendo* that California retains some vestigial merger requirement, it is clearly minimal, and at most requires only *some* connection to a document or tangible object—not representation of the owner's intangible interest in the strict *Restatement* sense." (emphasis in original)).

61. *See id.* at 1033–34 ("We agree that the [domain name database] is a document (or perhaps more accurately a collection of documents). . . . That it is stored in electronic form rather than on ink and paper is immaterial.").

62. *See id.* at 1036 ("The evidence supported a claim for conversion.").

common law does not stand idle while the people give away the property of others."[63]

B. The Contractually Created Right Theory: Digital Assets Cannot Be Owned

Just as *Kremen* stands for the proposition that domain names are property, *Network Solutions, Inc. v. Umbro International, Inc.*[64] represents the legal theory that domain names are not property.[65] In *Umbro*, plaintiff Umbro International, Inc. (Umbro) sought to garnish thirty-eight domain names held by defendant Network Solutions, Inc. (NSI).[66] Umbro previously obtained a judgment against a debtor in an unrelated bankruptcy action, and thereafter instituted this garnishment proceeding against NSI to collect on the debtor's domain names held by NSI.[67] Umbro sought a court order requiring NSI to begin the process of preparing the domain names for a sheriff's sale.[68] NSI responded to Umbro's lawsuit by claiming that it did not own any of the debtor's property.[69] NSI argued that the domain names were contractually created rights, which arose from NSI's contractual relationship with the debtor; thus, the domain names were not property capable of garnishment.[70]

The Supreme Court of Virginia agreed with NSI and determined that the intangible domain names were created solely because of a contractual relationship, and, thus, incapable of

---

63. *Id.*

64. 529 S.E.2d 80 (Va. 2000).

65. *See* Milton L. Mueller & Farzaneh Badiei, *Governing Internet Territory: ICANN, Sovereignty Claims, Property Rights and Country Code Top-Level Domains*, 18 COLUM. SCI. & TECH. L. REV. 435, 475 (2017) (explaining that *Umbro* has become one of the "most commonly cited" cases to prove that domain names are service contracts).

66. *See* Network Sols. Inc. v. Umbro Int'l, Inc., 529 S.E.2d 80, 81 (Va. 2000) ("In this case of first impression, we address the issue whether a contractual right to use an Internet domain name can be garnished.").

67. *Id.*

68. *Id.*

69. *Id.*

70. *Id.*

garnishment.[71] Because the debtor's rights to the domain names did not exist "separate and apart from" NSI's services to the debtor, the court deemed the domain names the but-for product of a contract.[72] Although the court agreed that the registrant gained the right to use the domain names upon registration, the right to use the domain names was "inextricably linked" to NSI's services.[73] Therefore, because garnishment proceedings are limited to liabilities owed, and service contracts are not within the statutory definition of the term "liabilities," the court reasoned that Umbro could not garnish NSI's domain names.[74]

Umbro stands for the proposition that domain names, and intangible property generally, are the product of a contract between the digital asset user and the digital asset provider.[75] Remarkably, NSI itself acknowledged and conceded that domain names constitute an intangible property during oral argument.[76] Although the court briefly analyzed the "contractually created right" versus "intangible property" argument, it dismissed NSI's oral argument concession and explained that classifying domain names as a type of property was not dispositive of the case.[77] The

---

71. *See id.* at 86 ("A contract for services is not 'a liability' as that term is used in § 8.01–511 and hence is not subject to garnishment.").

72. *See id.* ("[W]hatever contractual rights the judgment debtor has in the domain names at issue in this appeal, those rights do not exist separate and apart from NSI's services. Therefore . . . a domain name registration is the product of a contract for services between the registrar and registrant.").

73. *See id.* ("[W]e agree with Umbro that a domain name registrant acquires the contractual right to use a unique domain name for a specified period of time. However, that contractual right is inextricably bound to the domain name services that NSI provides.").

74. *See id.* ("[A] contract for services is not 'a liability' as that term is used in § 8.01–511 and hence is not subject to garnishment.").

75. *See* Mueller & Badiei, *supra* note 65, at 475 (explaining why *Umbro* has become "one of the cases most commonly cited to prove that domain names are services").

76. *See Umbro*, 529 S.E.2d at 86 ("[W]e must point out that NSI acknowledged during oral argument before this Court that the right to use a domain name is a form of intangible personal property.").

77. *See id.* at 770 ("However, NSI's acknowledgement is not dispositive of this appeal. Likewise, we do not believe that it is essential to the outcome of this case to decide whether the circuit court correctly characterized a domain name as a 'form of intellectual property.'").

court made clear that it did not garnish NSI's domain names because it feared that doing so would make practically any service contract garnishable.[78]

The *Umbro* case garnered a significant amount of criticism not for its holding, but for what the court failed to address.[79] Although *Kremen* plainly stands for the proposition that property rights exist in domain names,[80] *Umbro*'s substantive holding is *not* that domain names are contractually created rights.[81] The only legal conclusion *Umbro* drew is that domain names do not fall within the definition of "liability" as an element of the Virginia garnishment statute.[82] The court in *Umbro* briefly discussed only the property status of domain names in dicta when noting that NSI conceded that domain names were intangible property at oral argument.[83] Even though *Umbro* casually observed that a domain name represented a contractual right, the court never explicitly stated that domain names are not intangible property.[84] The court in *Umbro* even attempted to back away from making any definitive statements regarding domain name property rights (or lack

78. *See id.* at 771 ("If we allow the garnishment of NSI's services in this case because those services create a contractual right to use a domain name, we believe that practically any service would be garnishable.").

79. *See* Juliet M. Moringiello, *Seizing Domain Names to Enforce Judgments: Looking Back to Look to the Future*, 72 U. CIN. L. REV. 95, 97, 108 (2003) (calling *Umbro* a "red herring" case because it did not expressly hold that a domain name is not property).

80. *See* Kremen v. Cohen, 337 F.3d 1024, 1030 (9th Cir. 2003) ("Kremen therefore had an intangible property right in his domain name . . . .").

81. *See* Daniel Hancock, Note, *You Can Have It, But Can You Hold It?: Treating Domain Names as Tangible Property,* 99 KY. L.J. 185, 192–93 (2011) ("*Umbro* is often cited for the proposition that a domain name is simply a contractual arrangement and therefore cannot be a property right. This assertion is a misreading of the case.").

82. *See* Moringiello, *supra* note 79, at 108 ("The court simply said that a domain name did not constitute a 'liability' for the purpose of the Virginia garnishment statute.").

83. *See* Network Sols., Inc. v. Umbro Int'l, Inc., 529 S.E.2d 80, 86 (Va. 2000) ("Initially, we must point out that NSI acknowledged during oral argument before this Court that the right to use a domain name is a form of intangible personal property.").

84. *See id.* at 770 ("[W]e agree with Umbro that a domain name registrant acquires the contractual right to use a unique domain name for a specified period of time.").

thereof), noting that whether or not domain names constitute intangible property was not essential to the outcome of the case.[85]

C. Comparing the Intangible Property Theory to the Contractually Created Right Theory

Kremen and *Umbro* represent the two prevailing views on digital property's status as either intangible property or a contract for services.[86] The Ninth Circuit's opinion in the *Kremen* case stands for the theory that a digital asset is an intangible property owned by the user.[87] And although the Supreme Court of Virginia in *Umbro* never explicitly said so, the *Umbro* case stands for the theory that a digital asset is the product of a contract entered into between a user and a digital asset provider.[88]

Kremen and *Umbro*'s different outcomes are better understood when comparing the two distinguishing factors that led to their contrasting outcomes: (1) the unique parties to each case and (2) the different laws applied in each case. *Kremen* involved sympathetic plaintiff Gary Kremen, a "geek-turned-entrepreneur" who thought he hit the jackpot when he became the "proud owner" of sex.com (implying from the outset that domain names could be owned as property).[89] Kremen, unable to collect any of his initial $65 million judgment against domain thief Stephen Cohen (on account of Cohen fleeing the country), sued the deep-pocketed domain name provider responsible for carelessly transferring his domain to Cohen.[90]

---

85. *See id.* ("[W]e do not believe that it is essential to the outcome of this case to decide whether the circuit court correctly characterized a domain name as a form of 'intellectual property.'").

86. *See* Mueller & Badiei, *supra* note 65, at 472–73 (describing the property status of domain names as "less than settled" after twenty years of debate).

87. *See* Hancock, *supra* note 81, at 194–95 (calling the *Kremen* case illustrative of the view the domain names are intangible property).

88. *See id.* at 191–92 (explaining that *Umbro* represents the view that domain names are primarily contractual rights).

89. *See Kremen*, 337 F.3d at 1026–28 (describing Gary Kremen as computer geek who beat the hordes of NASDAQ day traders to become "the proud owner of sex.com").

90. *See id.* at 1035 ("Kremen never did anything. It would not be unfair to

Umbro involved unsympathetic plaintiff Umbro International, a multinational sporting equipment manufacturer, who tried to gain control of umbro.com from a "classic domain name pirate"[91] who held the "contractual right to use" the domain name (implying from the outset that the domain names were the but-for product of a contractual relationship).[92] Umbro International, which had already received the prized umbro.com domain as part of the original default judgment against the cybersquatter, pursued garnishment of the domain names solely to pay off its attorney's fees.[93]

Kremen had his domain name involuntarily transferred from him, needed the money, and had run out of legal options.[94] Conversely, Umbro International, a successful corporation, sought possession of a domain name it never previously owned or lost, and could likely absorb the relatively small amount of attorney's fees it sought to garnish.[95] It is therefore unsurprising that the *Kremen* court awarded down-on-his-luck Gary Kremen recourse against the culpable defendant,[96] while the *Umbro* court declined to award Umbro International the domain names to pay off its attorney's fees.[97]

---

hold Network Solutions responsible and force it to try to recoup its losses by chasing down Cohen. This, at any rate, is the logic of the common law, and we do not lightly discard it.").

91. *See* Umbro Int'l, Inc. v. 3263851 Canada, Inc., 48 Va. Cir. 139, 140 (Va. Cir. Ct. 1999) (describing the judgment debtor who owned umbro.com as a "classic domain name pirate").

92. *See Umbro*, 529 S.E.2d at 81 ("[W]e address the issue whether a contractual right to use an Internet domain name can be garnished.").

93. *See* Moringiello, *supra* note 79, at 105 ("Like many judgment debtors, Canada, Inc. did not write a check to Umbro, so like many judgment creditors, Umbro was forced to find property against which to enforce its judgment.").

94. *See* Kremen v. Cohen, 337 F.3d 1024, 1035 (9th Cir. 2003) ("Kremen never did anything. It would not be unfair to hold Network Solutions responsible and force *it* to try to recoup its losses by chasing down Cohen. This, at any rate, is the logic of the common law, and we do not lightly discard it." (emphasis in original)).

95. *See* Network Sols., Inc. v. Umbro Int'l, Inc., 529 S.E.2d 80, 81 (Va. 2000) (describing Umbro International's default judgment regarding umbro.com against 3263851 Canada).

96. *See Kremen*, 337 F.3d at 1036 ("The evidence supported a claim for conversion, and the district court should not have rejected it.").

97. *See Umbro*, 529 S.E.2d at 88 ("Even though the Internet is a 'new avenue of commerce,' we cannot extend established legal principles beyond their

A second important distinction between *Kremen* and *Umbro* lies in the different legal doctrines at play within each case. Gary Kremen's conversion claim was based on the common law tort, a necessary element of which was the court's determination that domain names constitute intangible property.[98] The flexible common law basis of Kremen's conversion claim gave the court leeway to determine an equitable outcome.[99]

In contrast, Umbro International's garnishment claim was based on a Virginia statute that did not require the court to determine whether domain names constitute intangible personal property.[100] *Umbro*'s rigid statutory basis constrained the court to solely determining whether a domain name was within the definition of a "liability" under the Virginia garnishment law.[101] In short, the *Kremen* court had to declare that domain names

---

statutory parameters. . . . For these reasons, we will reverse the judgment of the circuit court, dismiss the garnishment summons, and enter final judgment in favor of NSI." (quoting Intermatic Inc. v. Toeppen, 947 F. Supp. 1227, 1229 (N.D. Ill. 1996))).

98. *See Kremen*, 337 F.3d at 1029 (explaining that the California common law tort of conversion required the plaintiff to show ownership or a right to possession of property, wrongful disposition of the property, and damages).

99. *See id.* at 1036 (explaining that the court will "apply the common law until the legislature tells us otherwise. And the common law does not stand idle while people give away the property of others").

100. *See Umbro*, 529 S.E.2d at 85 (describing garnishment in Virginia as "a creature of statute unknown to the common law, and hence the provisions of the statute must be strictly satisfied").

101. *See* Moringiello, *supra* note 79, at 105 ("Garnishment, an action that did not exist at common law, is a creature solely of statute. . . . The Virginia garnishment statute is specific as to what types of property it covers and under the statute, only a 'liability' to the judgment debtor can be garnished.").

constitute intangible property to reach an equitable outcome,[102] while the *Umbro* court did not.[103]

D. The Evolution of Cybertrespass

Fifteen years after *Kremen* and *Umbro*, the question of whether intangible property can be converted or trespassed upon remains far from settled.[104] However, *Kremen*'s intangible property

---

102. *See Kremen*, 337 F.3d at 1036

> The district court thought there were "methods better suited to regulate the vagaries of domain names" and left it "to the legislature to fashion an appropriate statutory scheme." The legislature, of course, is always free (within constitutional bounds) to refashion the system that courts come up with. But that doesn't mean we should throw up our hands and let private relations degenerate into a free-for-all in the meantime. We apply the common law until the legislature tells us otherwise. And the common law does not stand idle while people give away the property of others.

(internal citation omitted).

103. *See Umbro*, 529 S.E.2d at 88 ("Even though the Internet is a 'new avenue of commerce,' we cannot extend established legal principles beyond their statutory parameters. . . . For these reasons, we will reverse the judgment of the circuit court, dismiss the garnishment summons, and enter final judgment in favor of NSI." (quoting Intermatic Inc. v. Toeppen, 947 F. Supp. 1227, 1229 (N.D. Ill. 1996))).

104. *See Kremen*, 337 F.3d at 1030–35 (explaining what constitutes an intangible personal property and determining that an intangible personal property can be the basis for a conversion claim); Thyroff v. Nationwide Mut. Ins., 460 F.3d 400, 405 n.2 (2d Cir. 2006) (explaining that although it "is unclear and unresolved" whether electronic data constitutes intangible property, the *Kremen* theory is one possible solution to the issue at hand); Emke v. Compana, L.L.C., No. 3:06-CV-1416-L, 2007 WL 2781661, at *5 (N.D. Tex. Sept. 25, 2007) (explaining that a claim of conversion of a domain name depends on what state law is applied); Dethmers Mfg. Co., Inc. v. Automatic Equip. Mfg., 23 F. Supp. 2d 974, 1006–07 (N.D. Iowa 1998) (surveying state caselaw to decide that Nebraska law might allow a claim for conversion of an unpatented idea); Curtis Mfg. Co. v. Plasti-Clip Corp., 888 F. Supp. 1212, 1233–34 (D.N.H. 1994) (holding that the plaintiff could make a claim for conversion of an idea). *But see* Kaempe v. Myers, 367 F.3d 958, 963 (D.C. Cir. 2004) ("[W]e conclude that it remains unclear whether D.C. law would permit an action for conversion of patent rights. The D.C. courts have never ruled on whether, or under what circumstances, intangible property of this nature can be the subject of a suit for conversion."); *In re* TJX Co. Retail Sec. Breach Litig., 527 F. Supp. 2d 209, 211 (D. Mass. 2007) (determining that Massachusetts law does not support a claim for conversion of intangible account data); Famology.com Inc. v. Perot Sys. Corp., 158 F. Supp. 2d 589, 591 (E.D. Pa. 2001) (explaining that because domain names are not tangible personal property, the plaintiff could not bring a conversion action under Pennsylvania

theory is spreading beyond domain name cases, as courts have recognized websites,[105] trademarks,[106] licenses,[107] investor lists,[108] and even expressed ideas[109] as forms of intangible property.

Because the internet's various equipment and virtual facilities are "not by any stretch of the imagination real property," the technological revolution forced courts and legal scholars to reevaluate the property laws governing the various digital devices that make up the internet.[110] The digital devices that constitute the internet are a "new" form of chattel, so it is logical that the law of trespass to chattels and conversion evolved to govern these devices.[111] The *Restatement (Second) of Torts* provides the classic language of an actionable trespass to chattels claim:

---

law).

105. *See* Margae, Inc. v. Clear Link Tech., 620 F. Supp. 2d 1284, 1288 (D. Utah 2009) (explaining that a website is personal property because it "has a physical presence on computer drive, causes tangible effects on computers, and can be perceived by the senses").

106. *See* English & Sons, Inc. v. Straw Hat Rest., Inc., 176 F. Supp. 3d 904, 921 (N.D. Cal. 2016)

> Trademarks, service marks, trade names, and much of the other intellectual property at issue here, meet this test. These can be precisely defined, exclusively possessed and controlled, and they can be the subject of a legitimate claim to such exclusivity. Under *Kremen*, then, such intellectual property should normally be proper objects of conversion.

107. *See* M.C. Multi-Family Dev., L.L.C. v. Crestdale Assoc., Ltd., 193 P.3d 536, 543 (Nev. 2008) ("[W]e conclude that a contractor's license is intangible personal property that may be converted under Nevada law.").

108. *See* Shmueli v. Corcoran Grp., 802 N.Y.S.2d 871, 876 (N.Y. Sup. 2005) ("The court, therefore, finds that plaintiff's computerized client/investor list is convertible property.").

109. *See* Astroworks, Inc. v. Astroexhibit, Inc., 257 F. Supp. 2d 609, 618 (S.D.N.Y. 2003) ("Although an idea alone cannot be converted, the 'tangible expression or implementation of that idea' can be." (quoting Matzan v. Eastman Kodak Co., 134 A.D.2d 863, 864 (N.Y. App. Div. 1987))).

110. *See* Richard A. Epstein, *Cybertrespass*, 70 U. CHI. L. REV. 73, 76 (2003) (explaining how the rise of the internet has caused a "rethinking of the property relations governed by the common law of trespass").

111. *See id.* ("[T]he focus of emphasis shifts because the various equipment and facilities that make up the internet are not by any stretch of the imagination real property. Rather, they are a new form of chattel, which are presumptively governed by the law of trespass to chattels.").

> One who commits a trespass to a chattel is subject to liability to the possessor of the chattel if, but only if,
>
> (a) he dispossesses the other of the chattel, or
>
> (b) the chattel is impaired as to its condition, quality, or value, or
>
> (c) the possessor is deprived of the use of the chattel for a substantial time, or
>
> (d) bodily harm is caused to the possessor, or harm is caused to some person or thing in which the possessor has a legally protected interest.[112]

The earliest virtual trespass to chattels (cybertrespass) cases involved unauthorized intrusions via the internet upon computer equipment.[113] These intrusions were serious enough to either overload the plaintiffs' computers and cause them to crash or crowd their hard drives' limited space with e-mails and burden the system owner with the task of deleting them.[114] More recently, virtual trespass to chattels cases have involved plaintiffs bringing claims based on trespass to intangible personal properties, such as social media accounts[115] and e-mails.[116]

---

112. RESTATEMENT (SECOND) OF TORTS § 218 (AM. LAW. INST. 1965).

113. *See, e.g.*, eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1063, 1071 (N.D. Cal. 2000) (granting eBay a preliminary injunction against Bidder's Edge web spiders based on a trespass to chattels claim even though Bidder's Edge software occupied, at most, between 1.11% and 1.53% of eBay's servers); Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548, 550–51 (E.D. Va. 1998) (finding the defendant liable for trespass to chattels for sending unauthorized bulk e-mails); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1027–28 (S.D. Ohio 1997) (granting the plaintiff a preliminary injunction to stop defendant's spam e-mails under a trespass to chattels theory). *But see* Intel Corp. v. Hamidi, 71 P.3d 296, 309 (Cal. 2003) (denying Intel's trespass to chattel claim because Hamidi's mass e-mails did not physically damage Intel's servers).

114. *See CompuServe*, 962 F. Supp. at 1028 ("High volumes of junk e-mail devour computer processing and storage capacity, slow down data transfer between computers over the Internet by congesting the electronic paths through which the messages travel, and cause recipients to spend time and money wading through messages that they do not want.").

115. *See* Salonclick LLC v. SuperEgo Mgmt. LLC, 16 Civ. 2555 (KMW), 2017 WL 239379, at *4 (S.D.N.Y. Jan. 18, 2017) (establishing that social media accounts are intangible personal property capable of being the subject of a conversion action, but dismissing the plaintiff's trespass to chattels action because the social media account itself did not suffer injury as a result of defendant's trespass).

116. *See* Porters Bldg. Ctrs., Inc. v. Sprint Lumber, No. 16-06055-CV-SJ-ODS,

Although text messages are a different form of digital communication from e-mails,[117] two recent opinions determining that e-mails constitute intangible personal property could outline the legal framework courts will apply to disputes over text messages in future cases.[118] In *Porters Building Centers, Inc. v. Sprint Lumber*,[119] a Missouri federal district court determined that if an intangible property has a connection to tangible property, the intangible property is a chattel capable of being the subject of a trespass to chattels action.[120] The court then explained that e-mails are a "chattel" because e-mail communications are connected to tangible servers stored in physical data centers.[121] After determining that e-mails constitute a "chattel," the court concluded that the plaintiff had a valid trespass to chattels claim against the defendant for improperly accessing and reading his personal e-mails.[122]

As well, in *Skapinetz v. CoesterVMS.com Inc.*,[123] a Maryland federal district court determined that e-mails, while not a traditional form of property, constitute "digital" property nonetheless.[124] This case again concerned a client's improper

---

2017 WL 4413288, at *15 (W.D. Mo. Oct. 2, 2017) (establishing that e-mails are intangible personal property, and thus a chattel, because the e-mail communication is connected to a tangible server, and thus allowing plaintiff's trespass to chattels claim to survive summary judgment).

117. *Supra* Part II.B.

118. *See Porters Bldg. Ctrs.*, 2017 WL 4413288, at *11 (finding that e-mails constitute intangible personal property because personal property can be intangible if there is a connection to tangible property, and the e-mail "communications are connected to something tangible—i.e., Google's servers").

119. No. 16-06055-CV-SJ-ODS, 2017 WL 4413288 (W.D. Mo. Oct. 2, 2017).

120. *See id.* at *11 ("The Court concludes Missouri courts would find a trespass to chattel claim includes an email communication when the email communication is connected to a tangible object, such as a server.").

121. *See id.* ("The Court takes judicial notice that Google stores its customers' email communications on servers. . . . Accordingly, [the plaintiff's] email communications are connected to something tangible—i.e., Google's servers.").

122. *See id.* (concluding that because a "chattel" extends to intangible property when the intangible property is connected to a tangible object, the plaintiff could maintain his trespass to chattels action against the defendant).

123. No. PX-17-1098, 2018 WL 805393 (D. Md. Feb. 9, 2018).

124. *See id.* at *4 ("Although email accounts and electronic communications are not tangible property in the traditional sense, many courts have recognized

access to a former employer's personal Gmail account.[125] After finding that e-mails constitute digital property, the court proceeded to determine that Georgia law allowed for both trespass to chattels claims and conversion claims involving intangible personal property such as e-mails.[126] By extension, the courts' reasoning in *Porters Building Centers* and *Skapinetz* could just as easily have applied to a case involving improper access to an iMessage account.

In sum, intangible property law has evolved beyond *Kremen*'s domain names to encompass a diverse group of digital assets. Courts are increasingly receptive to plaintiffs bringing property-based claims when their digital assets are trespassed upon or stolen. But, when plaintiffs do not bring these property-based causes of action, the judiciary defaults to *Umbro*'s "contractually created right" theory when dealing with digital assets,[127] as Part IV will show.[128]

IV. The Law Does Not Protect Text Messages

A. The Judiciary Does Not Protect Text Messages: The iMessage Litigation

The cases discussed below, centering around the Apple text messaging application "iMessage," merit thorough analysis because they are the only instances in which the judiciary has analyzed disputes regarding iMessage delivery problems.[129] The cases do not analyze the disputes over missing and delayed text

---

claims for conversion or trespass to chattels involving digital 'property.'").

125. *See id.* ("Skapinetz pleads that Defendants committed the torts of trespass and conversion by accessing without authorization, and intermeddling with, Skapinetz's email accounts and electronic communications.").

126. *See id.* ("These facts, taken as true, plausibly establish that Defendants assumed and exercised the right of ownership over Skapinetz's email accounts, albeit briefly, and these actions were inconsistent with Skapinetz's property rights. Therefore, Defendant's Motion to Dismiss the common law claim for conversion (Count Four) is DENIED.").

127. *Supra* Part III.B.

128. *Infra* Part IV.A.

129. *Infra* Part IV.A.

messages as if they were property trespassed upon or stolen.[130] Instead, the cases treat the disputes over text message delivery as a contractual dispute, harkening back to *Umbro*'s analysis of the specific terms of the contractual agreement.[131]

The iMessage litigation attracted a fair amount of publicity[132] because many former iPhone users experienced, and continue to experience,[133] similar iMessage disruptions after switching to a non-Apple device.[134] iMessage, Apple's proprietary text messaging service, is available only on Apple devices, and Apple works hard to keep it that way.[135] This strategy seems to work for Apple, as iPhone users often cite iMessage as the sole reason they refrain

---

130. *Infra* Part IV.A.

131. *Infra* Part IV.A.

132. *See* Christina Bonnington, *Apple Hit with Federal Lawsuit Over iMessage Delivery Issues*, WIRED (Nov. 11, 2014, 7:55 PM), https://www.wired.com/2014/11/apple-lawsuit-imessages/ (last visited Mar. 19, 2019) (detailing the lawsuit a former iPhone user brought against Apple for interfering with the delivery of iMessage text messages after the former iPhone user switched to an Android phone) (on file with the Washington and Lee Law Review).

133. *See, e.g.*, Terry Storch (@TerryStorch), TWITTER (Dec. 14, 2016), https://twitter.com/TerryStorch/status/805540549361070080 (last visited Mar. 19, 2019) ("The transition from iPhone to Android is still rough because of iMessage. As hard as you try, messages still get lost in the Interwebs.") (on file with the Washington and Lee Law Review); Lucocis, *After Almost 18 Months of Being on Android, I Still Have Problems Because of iMessages*, REDDIT (May 26, 2016),
https://www.reddit.com/r/Android/comments/40np11/after_almost_18_months_of_being_on_android_i/ (last visited Mar. 19, 2019) (describing a former iPhone user's struggle with losing text messages after switching to an Android device) (on file with the Washington and Lee Law Review).

134. *See* Damon Beres, *Apple Trapped Me on iOS—Perhaps Forever*, MASHABLE (Oct. 4, 2017), https://mashable.com/2017/10/04/the-iphone-owns-my-soul/ (last visited Mar. 19, 2019) ("If you switch to Android from iOS, I can nearly guarantee that you will miss texts from people you care about, and you may not be able to figure out how to fix it, exactly.") (on file with the Washington and Lee Law Review).

135. *See* Chance Miller, *This App Claims to Bring iMessage Support to Android, But Don't Expect It To Last*, 9TO5MAC (Dec. 12, 2017, 3:39 PM), https://9to5mac.com/2017/12/12/imessage-support-on-android-app/ (last visited Mar. 19, 2019) ("As has been the case with previous services that claim to add iMessages support to Android, you shouldn't expect this one to last for long. Apple generally does a good job of cracking down on these sorts of applications.") (on file with the Washington and Lee Law Review).

from switching to a non-Apple cellular device.[136] Even if Apple's self-contained technological ecosystem works fine for those who stick to Apple products, those who manage to escape Apple's "walled garden" soon find that making the switch is more painful than expected.[137]

1. Does Withholding Text Messages Amount to Tortious Interference with Contract?

Moore v. Apple, Inc.[138] involved a plaintiff who claimed she failed to receive iMessage text messages after she switched from an Apple iPhone to an Android device.[139] Adrienne Moore, who switched from an iPhone to a Samsung device running Android operating software, sued Apple because she failed to receive "countless text messages sent to her from Apple device users."[140]

---

136. *See, e.g.*, Patrick Holland, *iPhone's Blue Bubble Won't Let Me Stray to the Galaxy S8*, CNET (Apr. 21, 2017, 6:00 AM), https://www.cnet.com/news/why-the-iphones-blue-bubble-keeps-me-from-going-android/ (last visited Mar. 19, 2019) ("So if iMessage doesn't hop ship to Android, then I probably won't either.") (on file with the Washington and Lee Law Review); Damon Beres, *iMessage Is the Only Thing Keeping Me on an iPhone*, MASHABLE (Feb. 10, 2017), https://mashable.com/2017/02/10/imessage-is-keeping-me-on-iphone/#lKJYsF9EEmq8 (last visited Mar. 19, 2019) ("Apple has trapped me. iMessage, for the foreseeable future, will be the reason I stay on an iPhone, the reason I update my iOS software and ultimately the reason I buy a new iPhone when upgrade time rolls around.") (on file with the Washington and Lee Law Review); Lauren Goode, *iMessage is the Glue that Keeps Me Stuck to the iPhone*, VERGE (Oct. 10, 2016, 9:36 AM), https://www.theverge.com/2016/10/10/13225514/apple-iphone-cant-switch-pixel-android-imessage-addiction (last visited Jan. 28, 2019) ("Of course Apple wasn't going to allow iMessage to function on Android: iMessage is the glue that keeps people stuck to their iPhones and Macs.") (on file with the Washington and Lee Law Review).

137. *See* Victor Luckerson, *Apple Acknowledges iMessage Problems*, TIME (May 22, 2014, 4:32 PM), http://www.cnn.com/2014/05/22/tech/mobile/aple-imessage-problems-fix/index.html (last visited Mar. 19, 2019) ("But some people who switch from an iPhone to a non-Apple device have found it difficult to dissociate their phone numbers from iMessage. That leads to text messages from friends getting sucked up into Apple's database and disappearing.") (on file with the Washington and Lee Law Review).

138. 73 F. Supp. 3d 1191 (N.D. Cal. 2014).

139. *See id.* at 1195 ("Plaintiff replaced her iPhone 4 with a Samsung Galaxy S5. As a result of that switch, Plaintiff alleges that she has failed to received countless text messages sent to her from Apple device users.").

140. *See id.* (describing plaintiff Adrienne Moore's factual allegations

Moore reached out to Verizon, her cellular service provider, and Apple, and although both acknowledged that she was experiencing a known issue, their proposals to troubleshoot the problem were ultimately unsuccessful.[141] The California federal district court noted that "[Moore was] not the only former Apple device user to encounter the problem of undelivered text messages."[142] Despite her repeated attempts to rectify the situation and receive text messages from iPhone users, Moore continued to miss text messages.[143] Further, Moore stated that had she known about the undelivered text message problem at the outset, she would not have used iMessage or purchased an iPhone in the first place.[144]

Moore claimed that Apple's failure to deliver iMessages to her Android device (1) tortiously interfered with her Verizon contract and (2) violated California's Unfair Competition Law[145] (UCL) and California's Consumer Legal Remedies Act[146] (CLRA).[147] Although the court dismissed Moore's statutory UCL and CLRA claims, her tortious interference with contract claim survived the motion to dismiss.[148]

Moore claimed that (1) there was a valid contract between her and Verizon Wireless; (2) Apple had knowledge of this contract; (3) Apple intentionally acted to induce a breach or disruption of her contractual relationship with Verizon; (4) there was an actual breach or disruption of her contract; and (5) that there was

---

regarding her failure to receive text messages after switching from an iPhone to an Android device).

141. *Id.*

142. *Id.*

143. *Id.*

144. *Id.*

145. CAL. CIV. CODE § 1780(a) (West, Westlaw through Ch. 4 of 2019 Reg. Sess.).

146. CAL. BUS. & PROF. CODE § 17204 (West, Westlaw through Ch. 4 of 2019 Reg. Sess.).

147. *See Moore*, 73 F. Supp. 3d at 1195 (outlining Moore's causes of action).

148. *See id.* at 1205 ("[I]n summary, the Court denies Defendant's motion to dismiss Plaintiff's unlawful business practice UCL claim based on Plaintiff's tortious interference with contract claim. The Court grants Defendant's motion to dismiss Plaintiff's unfair business practice UCL claim with prejudice.").

resulting damage.[149] The court, in finding Moore sufficiently alleged her tortious interference with contract claim, determined that (1) a valid contract existed between Moore and Verizon which established the duty to send and receive text messages; (2) Apple had knowledge of Moore's contract with Verizon; (3) Apple knew about the undelivered text messages issue and did not alert Moore; and (4) Apple's iMessage application prevented Moore from fulfilling her contractual right to send and receive text messages.[150]

Following the court's decision to allow her case to proceed on the tortious interference with contract claim, Moore obtained documents during discovery which seemingly strengthened her claim.[151] Moore cited internal e-mails from Google showing the iMessage problem persisted and Apple's troubleshooting tips on solving the undelivered text message problem did not work.[152] What is more, she cited internal e-mails from Apple employees who were aware of the iMessage issue and apparently knew that Apple's guidance on fixing the problem was ineffective.[153]

Notwithstanding Moore's additional evidence of Apple's mishandling of the situation, the court later denied Moore's motion for class certification under Rule 23.[154] Although the court conceded that Moore satisfied the Article III standing requirement, the court denied her motion because her proposed class did not (1) satisfy Rule 23(a)'s commonality requirement or (2) satisfy Rule 23(b)'s predominance requirement.[155] Rule 23(a) requires a

---

149. *See id.* at 1202–03 (evaluating whether Moore's tortious interference with contract claim alleged enough facts to state a claim to relief that is plausible on its face).

150. *Id.*

151. *See* Moore v. Apple Inc., 309 F.R.D. 532, 537 (N.D. Cal. 2015) (discussing the plaintiff's evidence regarding Apple's awareness of the iMessage problem).

152. *See id.* ("Plaintiff cites internal emails from Google, Inc., from early 2015 indicating that the iMessage problem was not only persisting, but that the 'iMessage deregistration tool doesn't work.'" (internal citations omitted)).

153. *See id.* ("Plaintiff also points to Apple's own internal documents apparently discussing how Apple's 'so-called fixes' failed to address the disruptions in text message delivery.").

154. *See id.* at 549 (denying Moore's motion for class certification because her "proposed class includes, by definition, proposed class members who could not have suffered any injury and that individualized questions with respect to Defendant's liability will predominate over any common questions of law or fact").

155. *See id.* at 548 ("In sum, the Court is not persuaded that the question of

common contention that "must be of such nature that it is capable of classwide resolution—which means the determination of its truth or falsity will resolve an issue that is central to the validity of each one of the claims in one stroke."[156] Rule 23(b)'s predominance requirement "tests whether proposed classes are sufficiently cohesive to warrant adjudication by representation" and analyzes "the relationship between the common and individual issues in the case."[157]

The court held that Moore's proposed class did not meet Rule 23(a)'s commonality requirement because not every class member could claim they suffered the same contractual injury of not receiving text messages due to iMessage.[158] And Moore's proposed class did not meet Rule 23(b)'s predominance requirement because the contractual variations among class members would necessitate individualized inquiries into each claimant's contractual rights.[159]

The court's decision, albeit organized in separate analyses under Rule 23(a) and Rule 23(b), essentially hinged on a simple contractual issue: members of the proposed class each had different cellular service contracts containing different contractual provisions.[160] Because the members of the proposed class each had different cellular contracts, the court could not determine that each contract created the same contractual duty to send and receive text messages that Moore's did.[161] Consequently, because there were

---

whether iMessage is the cause of any contractual breach or interference satisfies the commonality requirement under Rule 23(a), much less the predominance requirement under Rule 23(b).").

156. *Id.* at 549.

157. *Id.* at 543.

158. *Id.* at 548–49.

159. *Id.* at 546–47.

160. *See id.* at 546

> [T]he Court finds that there are material variations in the proposed class members' wireless service agreements. These individualized issues will predominate because determining the fact of injury will require evaluating the particular terms of each individual class member's wireless service agreement, in order to determine whether Defendant actually caused a breach or interference with the agreement.

161. *See id.* ("[T]he Court could therefore not determine on a classwide or even carrier-wide basis whether individual class members were actually entitled to

likely members of the proposed class who did not have a contractual right to send and receive text messages, the proposed class was overbroad.[162]

The court's denial of class certification effectively ended Moore's case, and without the strength of a class action lawsuit, she withdrew her claim after presumably reaching an out-of-court settlement with Apple.[163]

2. Can Apple Intercept Text Messages Under the Wiretap Act?

In *Backhaut v. Apple, Inc.*,[164] plaintiffs Adam Backhaut, Joy Backhaut, and Kenneth Morris (the Backhaut plaintiffs) sued Apple for wrongfully intercepting and storing iMessages and preventing former iPhone users from receiving iMessages.[165] Adam Backhaut and Kenneth Morris switched from iPhones to non-Apple devices, and alleged that after making the switch they failed to receive text messages sent from iPhone users.[166] Joy Backhaut remained an iPhone user during the litigation, and she alleged that she sent her husband, Adam, text messages on her iPhone following his switch to a non-Apple device that he did not receive.[167]

The Backhaut plaintiffs claimed Apple's intercepting, storing, and withholding text messages violated the Stored

---

receive text messages.").

162. *Id.* at 543.

163. *See* Petitioner Adrienne Moore's Unopposed Motion to Withdraw Petition for Permission to Appeal Denial of Class Certification Pursuant to Fed. R. Civ. P. 23(f) at 1, Moore v. Apple, Inc., No. 15-80209 (9th Cir. Dec. 7, 2015) ("The parties have reached a resolution in this action, thereby mooting the petition to appeal.").

164. 74 F. Supp. 3d 1033 (N.D. Cal. 2014).

165. *See id.* at 1037 ("The gravamen of Plaintiffs' Complaint is that Apple wrongfully intercepts, stores, and otherwise prevents former Apple device users from receiving text messages sent to them from current Apple device users.").

166. *See id.* at 1038–39 (explaining that Adam Backhaut and Kenneth Morris purchased non-Apple devices after using iPhones and that both had difficulties receiving text messages from current iPhone users).

167. *See id.* at 1038 ("Following Adam Backhaut's switch, Plaintiff Joy Backhaut continued to send him text messages from her iPhone. On Joy Backhaut's phone, the word 'delivered' appeared under her messages to her spouse, but Adam Backhaut never received those messages.").

Communications Act,168 the Wiretap Act,169 California's Unfair Competition Law (UCL),170 and California's Consumers Legal Remedies Act (CLRA)171.172 The court quickly disposed of the Backhaut plaintiffs' Stored Communications Act claim for failure to state a claim, CLRA claim for lack of standing, and UCL claim for lack of standing and failure to state a claim.173 This left Apple's alleged Wiretap Act violations as the plaintiffs' sole surviving claim.174

The Backhaut plaintiffs alleged that Apple's intentional interception of iPhone users' text messages sent to former iPhone users violated the Wiretap Act.175 The Wiretap Act, which "protects communications in transit,"[176] bars the "interception" of "wire, oral, or electronic communications" and grants a private cause of action against any entity who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."[177] The California federal district court analyzed five factors to determine whether the Backhaut plaintiffs sufficiently alleged a Wiretap Act violation: (1) whether the plaintiffs alleged an actionable "interception"; (2) whether Apple's actions were within the "ordinary course of business exception"; (3) whether the plaintiffs alleged intent; (4) whether Apple's

168. 18 U.S.C. § 2701 (2012).

169. 18 U.S.C. § 2511.

170. CAL. BUS. & PROF. CODE § 17200 (West, Westlaw through Ch. 4 of 2019 Reg. Sess.).

171. CAL. CIV. CODE § 1750 (West, Westlaw through Ch. 4 of 2019 Reg. Sess.).

172. *See* Backhaut v. Apple, Inc., 74 F. Supp. 3d 1033, 1040 (N.D. Cal. 2014) (outlining the Backhaut plaintiffs' causes of action).

173. *See id.* at 1052 (listing the court's ruling on the Backhaut plaintiffs' Stored Communications Act claim, the CLRA claims, and the UCL claims).

174. *See id.* ("The Court DENIES Defendant's motion to dismiss Plaintiffs' Wiretap Act Claim.").

175. *See id.* at 1042 (summarizing the Backhaut plaintiffs' claims that gave rise to Apple's alleged Wiretap Act violations).

176. *See id.* (distinguishing the Stored Communications Act, which protects stored communications, from the Wiretap Act, which protects communications that are in transit).

177. 18 U.S.C. § 2511(1); *id.* § 2520.

alleged acts fell within the statutory good faith exception to liability; and (5) whether the plaintiffs consented to Apple's text message interceptions.[178]

First, the court determined that the Backhaut plaintiffs alleged an actionable "interception" under the Wiretap Act because the plaintiffs claimed that Apple intercepted and prevented text messages from being delivered using a "device" and the plaintiffs did not direct the messages toward Apple.[179] The plaintiffs' claimed "interception" was Apple's automated system of incorrectly categorizing messages sent to former iPhone users as iMessages instead of regular SMS/MMS text messages that were compatible with their non-Apple devices.[180] Second, the court found that the Apple's actions were not within the "ordinary course of business exception" under the Wiretap Act because the plaintiffs sufficiently alleged that Apple's "interception" neither facilitated nor was incidental to Apple's business of transmitting electronic communications.[181] Third, the court determined that the plaintiffs sufficiently alleged intent under the Wiretap Act because, in addition to outright claiming that Apple intentionally intercepted the text messages, the plaintiffs supported their allegation with information that Apple had been aware of the issue since 2012 and that Apple had even charged former iPhone users money to fix the problem.[182] And fourth, the court denied Apple's claim that its actions were covered by the "good faith exception" under the Wiretap Act because it found that Apple fundamentally misinterpreted the congressional intent behind the exception.[183]

---

178. *See Backhaut*, 74 F. Supp. 3d at 1042 (outlining Apple's five arguments as to why the Backhaut plaintiffs did not sufficiently state a Wiretap Act violation claim).

179. *See id.* (explaining the court's finding that the plaintiffs sufficiently alleged an actionable interception under the Wiretap Act).

180. *See id.* (clarifying the scheme the plaintiffs alleged Apple used to "intercept" text messages).

181. *See id.* at 1043 (explaining why Apple's claim that its actions in "intercepting" text messages did not "fall within the 'ordinary course of business' exception under the Wiretap Act").

182. *See id.* at 1044 (describing how the plaintiffs' allegation that Apple intended to intercept text messages satisfied the intent requirement under the Wiretap Act).

183. *See id.* at 1047 ("To the extent Apple contends that Congress intended to allow a good faith defense in reliance on any provision of the SCA and the Wiretap Act, despite the explicit language of § 2520(d)(3) and § 2707(e)(3), that argument

Thus, the Backhaut plaintiffs' Wiretap Act claim turned on the issue of the plaintiffs' consent to Apple intercepting their text messages. Under the Wiretap Act, it is lawful to intercept electronic communication when a party "to the communication has given prior consent to such interception."[184] Apple alleged that a provision of the Apple iOS iPhone operating system license agreement, which all iPhone users (including the Backhaut plaintiffs) agreed to before using their iPhone and iMessage software, evidenced the plaintiffs' prior consent to Apple's intercepting their text messages.[185] The relevant part of the provision read: "[t]o facilitate delivery of your iMessages and to enable you to maintain conversations across your devices, Apple may hold your iMessages in encrypted form for a limited period of time."[186]

At the outset, the court noted that the consent of one of the parties to the two-way text messaging communication was enough to preclude liability.[187] Because the Wiretap Act requires only "one of the parties to the communication" give prior consent, either the sender or the receiver of the text message could have consented to Apple's interception of the iMessages.[188] However, the Backhaut plaintiffs (with the exception of Joy) were former iPhone owners who were no longer bound by Apple's consent agreement, so the court's focus shifted to whether current iMessage users, who sent the text messages to the Backhaut plaintiffs, actually consented to Apple's intercepting their text messages.[189]

---

is unavailing.").

184. 18 U.S.C. § 2511(2)(d) (2012).

185. *See* Backhaut v. Apple, Inc., 74 F. Supp. 3d 1033, 1045 (N.D. Cal. 2014) (analyzing Apple's defense that the plaintiffs provided prior "consent to Apple's interception of their text messages").

186. *Id.*

187. *See id.* ("Apple is correct that consent of one of the parties to the communication, here the sender, would be sufficient to preclude liability under the Wiretap Act.").

188. 18 U.S.C. § 2511(2)(d).

189. *See Backhaut*, 74 F. Supp. 3d at 1045 ("The Court therefore addresses whether current iPhone/iMessage users, like Plaintiff Joy Backhaut, have consented to Apple's 'interception' of text messages intended for former Apple users.").

Although Apple argued that the above-quoted provision of its iOS agreement proved current iMessage users consented to text message interception, the court disagreed.[190] The court narrowly interpreted the provision at issue, explaining that "the license agreement only informs users that Apple may hold your iMessages in encrypted form for a limited period of time to facilitate delivery of your iMessages" to other iMessage users.[191] Noting that consent is "not an all-or-nothing proposition," the court determined that a reasonable user could deduce from the provision that Apple intercepts iMessages sent to other iMessage users, but does not intercept text messages sent to non-iMessage users.[192] For that reason, the court denied Apple's motion to dismiss the Wiretap Act claim based on consent.[193]

Even though the Backhaut plaintiffs' Wiretap Act claim survived Apple's motion to dismiss, the court would later deny the plaintiffs' Rule 23 motion for class certification.[194] The plaintiffs sought both certification of a damages class under Rule 23(b)(3) and certification of an injunctive relief class under Rule 23(b)(2).[195] The court refused to certify the plaintiffs' class because (1) the proposed class definition was unascertainable as there was no way to prove proposed class members would be capable of reliable self-identification, and (2) the individualized inquiry required to

---

190. *See id.* ("Apple relies solely on the bolded language in the iOS license agreement in arguing that current Apple device users have consented to its interception.").

191. *Id.*

192. *See id.* at 1046 (explaining that because consent is not absolute, "Apple may be correct that current Apple users consent to the interception of their messages for the purpose of 'facilitating' their delivery, however, it is less clear that users consent to interception where such interception would guarantee nondelivery").

193. *See id.* ("Taken as a whole, a reasonable user could conclude that Apple intercepts messages sent as iMesssages to other iMessage users, but that no such interception occurs if the text message cannot be sent as an iMessage. As such, the Court denies Defendant's motion to dismiss the Wiretap Act claim on the basis of consent.").

194. *See* Backhaut v. Apple Inc., No. 14–CV–02285–LHK, 2015 WL 4776427, at *1 (N.D. Cal. Aug. 13, 2015) ("Having considered the submissions of the parties, the relevant law, and the record in this case, the Court hereby DENIES Plaintiffs' motion for class certification.").

195. *See id.* at *3 ("Plaintiffs seek certification of a damages class under Rule 23(b)(3) and an injunctive relief class under Rule 23(b)(2).").

determine whether a proposed class member impliedly consented to Apple's alleged interception would predominate over any common questions of law or fact.[196]

Perhaps the most notable takeaway from the *Backhaut* litigation is the court's apparent waffling on the issue of consent to interception under the Wiretap Act.[197] After scarcely mentioning implied consent at the motion to dismiss stage,[198] the California federal district court reversed course and used implied consent to strike down the Backhaut plaintiffs' proposed class.[199] For a fact-finder to find implied consent to interception under the Wiretap Act, the fact-finder need not determine whether the text message user had specific knowledge of Apple's text message interceptions, but rather that the *surrounding circumstances* were enough to convincingly notify text message users of the interceptions.[200]

Borrowing its reasoning from *In re Google Inc. Gmail Litigation*[201] (hereinafter "the Gmail litigation"), the court determined that "broad disclosures" of information regarding the iMessage issue *might* be sufficient to put enough members of the proposed class on notice of the problem.[202] Because enough

196. *See id.* at *16 ("[T]he court finds that Plaintiffs . . . lack standing to seek certification of an injunctive relief class under Rule 23(b)(2). Furthermore, the Court finds that Plaintiffs' proposed damages class under Rule 23(b)(3) is unascertainable and that individualized issues with respect to consent predominate over any common issues.").

197. *See id.* at *15 ("Here, however, the predominance problems posed by Defendant's implied consent defense are distinct from the express consent defense Defendant raised at the motion to dismiss stage.").

198. *See* Backhaut v. Apple, Inc., 74 F. Supp. 3d 1033, 1045 (N.D. Cal. 2014) (explaining that consent under the Wiretap Act can be either express or implied, but it must be actual).

199. *See* Backhaut v. Apple Inc., No. 14–CV–02285–LHK, 2015 WL 4776427, at *15 (N.D. Cal. Aug. 13, 2015) ("[T]he Court does find that the need to determine, on an individual-by-individual basis, whether a proposed class member impliedly consented to any alleged interception would predominate over any common questions of law or fact.").

200. *See* Berry v. Funk, 146 F.3d 1003, 1011 (D.C. Cir. 1998) (finding that "consent can only be implied when the surrounding circumstances convincingly show that the party knew about and consented to the interception").

201. No. 13–MD–02430–LHK, 2014 WL 1102660 (N.D. Cal. Mar. 18, 2014).

202. *See id.* at *20 (explaining how "a fact-finder could find implied consent even based on broad disclosures").

members of the proposed class *might* have been on notice of the iMessage problem, those members' continued iMessage use (following possible notice) *might* mean they impliedly consented to the interception.[203] In the Gmail litigation, seven years of regular nationwide media coverage of Google's scanning customers' e-mails, coupled with a "panoply" of Google's disclosures on the issue, constituted "broad disclosures" on which the court based its finding of implied consent.[204] In contrast, the "broad disclosures" of information regarding the iMessage problem that the court in *Backhaut* relied on to find implied consent were tech blog posts, tech blog comments, forum postings and comments on Apple's website, and a disclosure Apple posted on its website warning users to deregister their iMessage before switching to a non-Apple device.[205]

In effect, the *Backhaut* court found that blog posts, forum posts, and a single disclosure on Apple's website were equivalent to seven years of nationwide media coverage and numerous corporate disclosures in creating a potential implied consent issue.[206] Because the implied consent issue necessitated an inquiry into the actual consent of each proposed class member, the court found that the consent issue predominated any common questions of law among class members and denied the *Backhaut* plaintiffs' motion for class certification.[207]

The Ninth Circuit recently upheld the *Backhaut* decision on appeal.[208] Interestingly, the Ninth Circuit sidestepped the entire

---

203. *See Backhaut*, 2015 WL 4776427, at *14–15 (reasoning that "broad disclosures" of news information might have been sufficient to put members of the proposed class on notice of the iMessage interceptions).

204. *See In re Gmail Litig.*, 2014 WL 1102660, at *18–20 (listing the sources of information disclosure that led the court to find that consent cannot be determined on a class-wide basis).

205. *See Backhaut*, 2015 WL 4776427, at *15 (listing the various sources of information available covering the iMessage delivery issues).

206. *See id.* (explaining that public information available concerning the iMessage issue might be sufficient to put iMessage users on notice because news articles were arguably evidence of implied consent in the Gmail litigation).

207. *See id.* ("In sum, the Court finds that the highly individualized and fact-specific inquiry required to determine whether a proposed class member impliedly consented to Defendant's alleged interception would predominate over any common questions of law or fact.").

208. *See* Backhaut v. Apple Inc., No. 15-17523, 723 Fed. Appx. 405, 407–408 (9th Cir. Jan. 29, 2018) (upholding the district court's decision to dismiss the

consent issue, and determined that text messages held in "temporary storage" are not intercepted under the Wiretap Act.[209] Additionally, the court found that the "misclassification" by the sender of a message as an iMessage (instead of a text message) to a former iPhone user caused the problem, and not Apple's faulty iMessage-to-text message handoff system.[210] Just as the judiciary has proven ineffective at protecting text message users' rights against corporate overreach, the Constitution is likewise inadequate at protecting their rights against government overreach.

B. The Fourth Amendment Does Not Protect Text Messages: The Third-Party Loophole

Our cell phones and constitutional law collide when law enforcement officials seek to search the contents of our cell phones as part of an arrest, investigation, or prosecution. Consider another scenario: on the day of Mark's high school senior prom, someone calls in a bomb threat to Mark's high school. Mark is sent home for the day along with everyone else, and much to his surprise the police soon show up at his front door prepared to arrest him for the bomb threat.

Seven months before the bomb threat, Mark texted his friend, "Prom this year will be the BOMB!" Following the bomb threat, Mark's cellular service provider's linguistics algorithms flagged Mark's text message for containing the words "prom" and "bomb," and Mark's third-party service provider quickly handed this text message off to the police.[211] Solely because of Mark's

---

plaintiffs' claims on summary judgment).

209. *See id.* ("[T]he message was no longer in transmission—it was in temporary storage—and so under *Konop* could not be 'intercepted' within the meaning of the Wiretap Act.").

210. *See id.* at 407 (finding that there was no interception, just a "misclassification [which] occurred when the recipient's phone number was first entered in the 'To' field by the user of the Apple product trying to send a message. This misclassification occurred before any message was sent, not 'during transmission' of a message").

211. *See* JOSHUA A. T. FAIRFIELD, OWNED: PROPERTY, PRIVACY, AND THE NEW DIGITAL SERFDOM 115 (1st ed. 2017) (outlining the process by which the

seven-month-old text to his friend, he just became the prime suspect in the bomb threat investigation. But how could the police read Mark's text messages if they had no probable cause to believe he called in the bomb threat?

Text messages, a protected "paper" under the Fourth Amendment,[212] may be searched and read by the police without probable cause because of the third-party doctrine.[213] The Fourth Amendment bans the government from conducting warrantless searches and seizures.[214] This ban on government action seeks to strike a balance between privacy and security.[215] In practice, the Fourth Amendment splits law enforcement conduct into two categories: police actions that require a warrant, and police actions that do not.[216] The police do not need a search warrant to monitor occurrences in public, but the police do need a search warrant to monitor your home or private mail because of the Fourth Amendment.[217]

The Constitution bars the government from warrantlessly searching content stored directly on your cell phone,[218] as it likely contains more sensitive information than your entire home.[219] However, because the Fourth Amendment restricts government action only under the state action doctrine, private third-party actors (e.g., non-government companies and individuals) are not

---

government obtains text messages from third parties).

212. U.S. CONST. amend. IV.

213. *See* FAIRFIELD, *supra* note 211, at 115 (explaining the logistics of the third-party doctrine).

214. *See* U.S. CONST. amend. IV ("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.").

215. *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 574 (2009) ("The Fourth Amendment's prohibition on unreasonable searches and seizures is premised on a balance between privacy and security.").

216. *See id.* ("To implement that balance, the Supreme Court has created two basic categories of law enforcement conduct: investigative steps that the Fourth Amendment regulates and those that it does not.").

217. *See id.* (comparing the actions the police need a search warrant for to the actions the police do not need a search warrant for).

218. *See* Riley v. California, 573 U.S. 373, 401–03 (2014) (extending the Fourth Amendment protection against search and seizures to data within a cell phone).

219. *See id.* at 398 (2014) ("[A] cell phone search would typically expose to the government far more than the most exhaustive search of a house.").

constitutionally barred from searching the contents of your cell phone.[220] Thus, the Constitution restricts the government from searching the contents of your cell phone, but there is no equivalent law that restricts the private sector from conducting a search that would be illegal if a government actor performed it. This inconsistency has been termed the "third-party loophole," or the "third-party doctrine."[221]

Under the third-party doctrine, an individual who voluntarily conveys information to a third party (e.g., a cellular service provider) maintains no reasonable expectation of privacy.[222] Put another way, if a consumer voluntarily reveals information to a business, the consumer takes the risk that the business will give that information to the government.[223] Normally, the government cannot search something someone reasonably expects to be private, but once someone conveys that interest to a third party, their reasonable expectation of privacy is lost.[224] Thus, the third-party loophole allows the government to freely obtain consumer electronic communications from cellular service providers that the government would not otherwise be able to gather without a warrant.[225]

Although courts historically applied the third-party doctrine to a discrete set of records-related categories,[226] in modern-day

---

220. *See* Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611, 613 (2015) (explaining that the Fourth Amendment does not stop private companies from conducting searches and seizures).

221. *See* FAIRFIELD, *supra* note 211, at 115–16 (discussing the third-party exception to data searches and naming it the "third-party loophole").

222. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

223. *See id.* at 745 (explaining that because the petitioner voluntarily conveyed information to a business, the "petitioner assumed the risk that the information would be divulged to police").

224. *See* United States v. Miller, 425 U.S. 435, 443 (1976) ("The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.").

225. *See* Brennan-Marquez, *supra* note 220, at 613 (discussing how the third-party doctrine enables the government to get around the Fourth Amendment's warrant requirement).

226. *See* United States v. Suarez-Blanca, No. 1:07–CR–0023–MHS/AJB, 2008

jurisprudence, the third-party doctrine has evolved into a single test: if any information is disclosed to a third party, then that information becomes public and it is not entitled to the protections afforded by the Fourth Amendment.[227] This has led to a drastic expansion of the government's ability to obtain information.[228] By analogy, the government previously used the third-party doctrine to read the address written on the outside of a sealed letter; now, the government uses the same doctrine to read the contents of the letter itself.[229]

Even if a user conveys information to a third party confidentially and under the assumption that the third party will use it for only limited purposes, the information nonetheless loses its Fourth Amendment protection.[230] For example, the third-party doctrine allows the government to, without a warrant, request the contents of e-mails sent through the Google's e-mail platform "Gmail," because Gmail users agreed to allow Google read the contents of their e-mails.[231] Gmail users might expect that Google will keep the contents of their e-mails confidential, but because

---

WL 4200156, at *8 (N.D. Ga. Apr. 21, 2008) (categorizing the third-party doctrine as applying to six situations: "(1) bank records; (2) credit card statements; (3) kilowatt consumption from electric utility records; (4) motel registration records; (5) cell phone records; and (6) employment records").

227. *See* Note, *If These Walls Could Talk: The Smart Home and the Fourth Amendment Limits of the Third Party Doctrine*, 130 HARV. L. REV. 1924, 1931 (2017) (explaining that the modern third-party doctrine "has calcified into a binary one, in which any information disclosed to a third party for any reason is public and does not merit Fourth Amendment protection").

228. *See* Kerr, *supra* note 215, at 587 (explaining how a common criticism of the third-party doctrine is that "it gives the government too much power").

229. *See id.* (comparing the government's past use of the third-party doctrine to the government's current use of the doctrine).

230. *See* United States v. McIntyre, 646 F.3d 1107, 1112 (8th Cir. 2011) ("[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by the third party to government authorities, even if the information is revealed to the third party confidentially and on the assumption that it will be used only for limited purposes.").

231. *See* GOOGLE, PRIVACY POLICY (2017), https://www.google.com/intl/en/policies/privacy/google_privacy_policy_en.pdf ("Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection.").

Gmail users allow Google to read the contents of their e-mails,[232] the government does not need a warrant to access the e-mails.[233]

Congress tried to define the scope of the Fourth Amendment's protections of electronic communications with the Stored Communications Act (SCA).[234] However, the SCA merely provides temporary Fourth Amendment protection of electronic communications stored on third-party servers.[235] Under the SCA, once text messages stored on a third-party server are greater than 180 days old, the government is no longer required to obtain a warrant with probable cause to access the text messages.[236] Apple, for instance, stores iPhone users' iMessages and SMS messages on its iCloud servers.[237] Consequently, after an iPhone user's text message is more than 180 days old, the SCA does not protect that text message, and the government may compel Apple to disclose the text message even though no warrant has been issued.[238]

---

232. *Id.*

233. *See* Note, *supra* note 227, at 1931 (using Google as an example of a situation in which "it is not difficult to imagine that one would want and expect to be able to keep some information private in certain respects but not in others").

234. *See* Achal Oza, Note, *Amend the ECPA: Fourth Amendment Protection Erodes as E-Mails Get Dusty*, 88 B.U. L. REV. 1043, 1072 (2008) ("Congress passed the ECPA in 1986 to draw clear lines as to where Fourth Amendment protection extends with emerging technologies.").

235. *See id.* at 1044–45 (explaining that digital messages stored on a third party server are no longer protected by the Fourth Amendment's probable cause requirement under the Electronic Communications Privacy Act after they are over 180 days old).

236. *See* 18 U.S.C. § 2703(a) (2012) ("A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b)."); *id.* (outlining how "[a] governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication" with delayed notice pursuant to Section 2705); *id.* § 2705 (describing the process the government can take to indefinitely delay notifying the customer whose electronic communications the government searched pursuant to § 2703(a)).

237. *See Privacy*, APPLE, https://www.apple.com/privacy/approach-to-privacy/ (last visited Mar. 19, 2019) ("iMessage and SMS messages are backed up on iCloud for your convenience, but you can turn iCloud Backup off whenever you want.") (on file with the Washington and Lee Law Review).

238. *See* Oza, *supra* note 234, at 1044–45 (explaining how once electronic communications are stored for greater than 180 days on a third-party server, the

In sum, as we store nearly our entire digital lives on third-party, cloud-based servers in one way or another,[239] the third-party loophole has crippled the Fourth Amendment's protection over stored communications.[240] Although this paints a bleak picture for consumers hoping to keep the government from intruding into their private text message inbox, a potential stopgap exists in an area of law much more ancient than the electronic devices and data at issue: property law.[241]

V. The Solution is Property Law

This Part argues that text messages constitute intangible personal property.[242] This leads to two separate practical outcomes: first, plaintiffs such as those in the *Moore* and *Backhaut* cases would have been successful had they sued Apple under property-based causes of action;[243] and second, text messages, as property, should receive increased Fourth Amendment protections against warrantless searches, thus closing the third-party loophole.[244]

A. Text Messages Are Property

Under *Kremen*, text messages constitute an intangible personal property if they are (1) "an interest capable of precise definition"; (2) "capable of exclusive possession or control"; and (3) there is a "legitimate claim to exclusivity."[245]

---

electronic communications are no longer protected by the ECPA's probable cause requirement).

239. *See* Daniel Martin, Note, *Dispersing the Cloud: Reaffirming the Right to Destroy in a New Era of Digital Property*, 74 WASH. & LEE L. REV. 467, 524 (2017) (discussing the proliferation of information stored on the cloud).

240. *See* Oza, *supra* note 234, at 1044–45 ("As more of our personal information is electronically stored on third-party servers, this exception threatens to nullify the Fourth Amendment.").

241. *See* FAIRFIELD, *supra* note 211, at 114 (arguing that the law of property trespass should pick up for third parties where the Fourth Amendment stops).

242. *Infra* Part V.A.

243. *Infra* Part V.B.

244. *Infra* Part V.C.

245. *See* Kremen v. Cohen, 337 F.3d 1024, 1030 (9th Cir. 2003) (outlining the

First, text messages are an interest capable of precise definition because the text within the message itself is precisely worded for the recipient.[246] Although there is not a theoretically finite amount of text messages in the same way there are a limited amount of domain names or plots of land, each text message sent is a unique interaction between the sender and receiver at the time and place of its sending that cannot be recreated by others.[247]

Second, text messages are capable of exclusive possession and control because cell phone owners have sole possession of the text messages they have sent and received on their own personal devices.[248] A cell phone owner has exclusive possession and control over the messages contained within their cell phone's text message application.[249]

Finally, text message owners have a legitimate claim to exclusivity over their text messages because encryption and phone security features protect the messages and ensure the content of the messages remains private between the sender and receiver.[250]

Some courts, in addition to applying some form of the *Kremen* test, also require the intangible personal property to have a basis in a tangible property.[251] This means that the digital "thing" has to have some sort of a connection to a physical object, but the owner

---

Ninth Circuit's three-part test to determine whether a digital object constitutes an intangible personal property).

246. *See* Moore v. Apple Inc., 309 F.R.D. 532, 536 (N.D. Cal. 2015) (explaining the process by which a user sends a text message to the recipient).

247. *See Kremen*, 337 F.3d at 1030 (determining that a domain name is a well-defined interest by likening it to "a share of corporate stock or a plot of land").

248. *See id.* (finding that a domain name owner has exclusive possession and control of the domain name because the domain name registrant alone makes the decision on what domain to purchase).

249. *Id.*

250. *See id.* ("[R]egistrants have a legitimate claim to exclusivity. Registering a domain name is like staking a claim to a plot of land at the title office. It informs others that the domain name is the registrant's and no one else's.").

251. *See, e.g.*, Porters Bldg. Ctrs., Inc. v. Sprint Lumber, No. 16-06055-CV-SJ-ODS, 2017 WL 4413288, at *10 (W.D. Mo. Oct. 2, 2017) ("[M]any courts have applied trespass to chattels to actions taken in cyberspace. But there is no consensus among the courts. Some courts found personal intangible property is chattel. Other courts concluded trespass to chattel, including a claim related to intangible property, must have a connection to tangible property.").

need not have control over the physical object.[252] Although this might be a tough element for other cloud-based forms of intangible property, such as e-mails, to overcome, text messages easily surpass this threshold. Text messages are connected to, and stored directly on, the one object everyone has within an arm's length at all times: cellular phones.[253] And if an argument is made that the text messages themselves are not stored within the phone but rather stored on servers scattered around the world (the "cloud"), it makes no difference, as the servers themselves are tangible property.[254]

Consequently, text messages constitute a form of intangible personal property. The recent uptick in federal courts finding that e-mails constitute personal property signals that it will not be long until courts determine that text messages are property.[255] With that in mind, would the iMessage plaintiffs have succeeded had they brought claims based on the theory that their text messages were their property?

B. Why the iMessage Plaintiffs Should Have Succeeded

The iMessage cases share similar facts: former iPhone users sued Apple, alleging that Apple interfered with their receiving text messages after they switched to a non-Apple cellular device.[256] The iMessage cases even share the same judge, as Judge Lucy H. Koh of the U.S. District Court for the Northern District of California

252. *See Kremen*, 337 F.3d at 1033 ("Assuming arguendo that California retains some vestigial merger requirement, it is clearly minimal, and at most requires only some connection to a document or tangible object—not representation of the owner's intangible interest in the strict Restatement sense.").

253. *See* Ellen Brait, *Smash It, Shred It, Wipe It: The Tom Brady Guide to Destroying Text Messages*, GUARDIAN (July 29, 2015, 12:47 PM), https://www.theguardian.com/technology/2015/jul/29/tom-brady-deflategate-destroy-text-messages-cellphone (last visited Mar. 19, 2019) (explaining how text messages are stored both on cell phones themselves and also stored on cellular service providers' servers) (on file with the Washington and Lee Law Review).

254. *Id.*

255. *Supra* notes 118–126 and accompanying text.

256. *See supra* notes 138–144 and accompanying text (discussing the *Moore* case's factual background); *supra* notes 164–167 and accompanying text (discussing the *Backhaut* case's factual background).

authored both opinions.[257] And, unfortunately, the iMessage cases also share similar results: the plaintiffs lost at the class certification stage.[258]

Would the outcome have been different if the plaintiffs pursued a trespass to chattels or conversion cause of action against Apple? This subpart applies the intangible personal property theory to the iMessage litigation's facts: first, the court would decide whether the plaintiffs had a valid trespass to chattels or conversion claim;[259] and second, the court would determine whether to certify the plaintiffs' proposed class action lawsuit.[260]

1. As Property, Text Messages Can Be Converted or Trespassed Upon

As established, text messages constitute a form of property under the Ninth Circuit's precedent in *Kremen*.[261] The hypothetical court would initially determine whether the text message property was taken (conversion) or disrupted (trespass to chattels).[262] Using the iMessage litigation as our facts, where Apple blocked former iMessage users from receiving text messages after the former users switched to non-Apple devices, the former iMessage users would likely prevail (at least individually) on both a trespass to chattels claim and a conversion claim against Apple.[263]

---

257. *See supra* notes 138–144 and accompanying text (discussing the *Moore* case's factual background); *supra* notes 164–167 and accompanying text (discussing the *Backhaut* case's factual background).

258. *See supra* note 163 and accompanying text (discussing the *Moore* case's conclusion following the court's refusal to certify the class); *supra* notes 208–210 and accompanying text (discussing the *Backhaut* case's conclusion following the plaintiffs' unsuccessful appeal).

259. *Infra* Part V.A.1.

260. *Infra* Part IV.A.2.

261. *Supra* Part IV.A.

262. *See* Porters Bldg. Ctrs., Inc. v. Sprint Lumber, No. 16-06055-CV-SJ-ODS, 2017 WL 4413288, at *10 (W.D. Mo. Oct. 2, 2017) (explaining how before the court can determine if a trespass to chattels occurred, the court must determine whether e-mails fall within the definition of a chattel).

263. *See supra* notes 138–144 and accompanying text (discussing the *Moore* case's factual background); *supra* notes 164–167 and accompanying text

Under California law, "a trespass to chattels claim lies where (1) an intentional interference with (2) the possession of personal property has (3) proximately caused injury."[264] First, the courts in the iMessage litigation found that the plaintiffs sufficiently alleged that Apple likely intended to slow down or delay the messages sent from iPhone users to former iPhone users because it was aware of the problem and did not act to fix it.[265] Second, Apple interfered with possession of the iMessage users' property because Apple's actions delayed and prevented the former iPhone owners from possessing and receiving their text messages.[266]

The third prong, whether Apple proximately caused injury by intercepting and withholding the text messages, is the most challenging to establish. In California, specifically in the context of a computer or digital system, "injury is adequately alleged where the plaintiff pleads that the purported trespass deprived plaintiff of the use of personal property for a substantial time."[267] The plaintiffs in the iMessage litigation never received the missing text messages from iMessage users who attempted to text message them after they switched to non-Apple devices.[268] Although Apple could argue that its iMessage deregistration system takes effect after forty-eight hours, the plaintiffs did not register for this system before switching to non-Apple devices, and thus the deregistration issue is moot.[269]

(discussing the *Backhaut* case's factual background).

264. Intel Corp. v. Hamidi, 30 Cal. 4th 1342, 1350–51 (Cal. 2003).

265. *See* Backhaut v. Apple, Inc., 74 F. Supp. 3d 1033, 1044 (N.D. Cal. 2014) ("Plaintiffs have alleged that Apple knowingly, intentionally, and deliberately intercepted text messages. On a motion to dismiss, these allegations are sufficient.").

266. *See* Moore v. Apple, Inc., 73 F. Supp. 3d 1191, 1195 (N.D. Cal. 2014) ("Plaintiff alleges that Apple failed to disclose that use of iMessage and Messages would result in undelivered messages if an iPhone user switched to a non-Apple device.").

267. Grace v. Apple Inc., No. 17-CV-00551, 2017 WL 3232464, at *11 (N.D. Cal. July 28, 2017).

268. *See Backhaut*, 74 F. Supp. 3d at 1038 ("Following Adam Backhaut's switch, Plaintiff Joy Backhaut continued to send him text messages from her iPhone. On Joy Backhaut's phone, the word 'delivered' appeared under her messages to her spouse, but Adam Backhaut never received those messages.").

269. *See Moore*, 73 F. Supp. 3d at 1196 ("Plaintiff noticed she was not receiving text messages she expected to receive from users of Apple devices. After this initial discovery, Plaintiff contacted her service provider, Verizon Wireless,

When Apple failed to deliver the text messages to the former iMessage users in the iMessage litigation, it injured the plaintiffs because it deprived them of the use of their property for a substantial time.[270] Thus, because Apple intentionally interfered with the former iMessage users' text messages and proximately caused injury, the plaintiffs in the iMessage litigation would have likely succeeded in their trespass to chattels claim against Apple.

To establish the tort of conversion, the iMessage plaintiffs must show (1) that they owned the text messages; (2) that Apple's actions constituted a wrongful disposition of a property right; and (3) damages.[271] As established above, text messages constitute intangible personal property, so the iMessage plaintiffs satisfy the first "property" prong. The iMessage plaintiffs should succeed in proving that Apple's interception of the text messages constituted a wrongful disposition of a property right, as the plaintiffs never received their text messages.[272] And the plaintiffs will satisfy the damages requirement because their cellular contracts guaranteed the plaintiffs the right to send text messages, and Apple's interference with the text messages deprived the plaintiffs of the "full benefit of [their] contractual bargain."[273] Thus, the iMessage plaintiffs would have likely succeeded had they brought a conversion cause of action against Apple.

---

which informed her that she needed to 'turn off' Messages on her old iPhone.").

270. *See Grace*, 2017 WL 3232464, at *13 (finding that the FaceTime plaintiffs satisfied the injury element because they sufficiently alleged "that Apple's disabling of FaceTime 'impaired the condition, quality, or value' of their iPhones" (quoting Fields v. Wise Media, LLC, No. C 12-05160 WHA, 2013 WL 5340490, at *4 (N.D. Cal. Sept. 24, 2013))).

271. *See* Kremen v. Cohen, 337 F.3d 1024, 1029 (9th Cir. 2003) ("To establish [conversion], a plaintiff must show ownership or right to possession of property, wrongful disposition of the property right and damages.").

272. *See Backhaut*, 74 F. Supp. 3d at 1038 (explaining how a plaintiff never received the missing text messages).

273. *See* Moore v. Apple, Inc., 73 F. Supp. 3d 1191, 1199 (N.D. Cal. 2014) ("Plaintiff alleges that Apple's interference with the receipt of her text messages deprived her of the full benefit of her contractual bargain with Verizon Wireless.").

2. The Final Step: Class Certification

Taking our hypothetical iMessage litigation to its conclusion, the final step, following the iMessage plaintiffs' successful individual trespass to chattels or conversion claims against Apple, would be the class certification stage. Judge Koh might well deny class certification again, as she has turned Rule 23(b)(3) damages class certification into a nearly impenetrable barrier for plaintiffs to break through.[274] However, the iMessage plaintiffs' novel property-based causes of action, combined with Judge Koh's comparative leniency toward Rule 23(b)(2) injunctive class certifications, gives the iMessage plaintiffs a realistic chance at clearing the class certification hurdle.[275] Moreover, injunctive relief would better serve the iMessage plaintiffs' goals, as the court could, in effect, force Apple to deliver the missing text messages to former iMessage users right away.[276] As the court already found that the iMessage litigants satisfied Article III standing, the court would analyze whether the plaintiffs met the requirements for an injunctive class under Rule 23(b)(2).[277]

To establish an injunctive class under Rule 23(b)(2), the iMessage plaintiffs must prove that they have suffered a "concrete and particularized" harm and that they are "subject to a likelihood of future injury."[278] Although the plaintiffs in *Backhaut* failed in

---

274. *See* Philips v. Ford Motor Co., No. 14-CV-02989-LHK, 2016 WL 7428810, at *23 (N.D. Cal. Dec. 22, 2016) (denying plaintiffs' proposed classes because they did not meet the Rule 23(b)(3) predominance requirement); *In re* Google Inc. Gmail Litig., No. 13– MD– 02430–LHK, 2014 WL 1102660, at *12 (N.D. Cal. Mar. 18, 2014) (finding that the plaintiffs did not meet "their burden of demonstrating that the proposed classes satisfy the [Rule 23(b)(3)] predominance requirement"); *In re* High-Tech Emp. Antitrust Litig., No. 11– CV–02509–LHK, 2013 WL 1352016, at *587 (N.D. Cal. Apr. 5, 2013) (denying plaintiffs' class certification because the proposed class did not meet the Rule 23(b)(3) predominance requirement).

275. *See In re* Yahoo Mail Litig., 308 F.R.D. 577, 601 (N.D. Cal. 2015) (granting plaintiffs' motion for an injunctive class certification under Rule 23(b)(2)).

276. *See* Robert H. Klonoff, *The Decline of Class Actions*, 90 WASH. U. L. REV. 729, 734 (2013) (explaining how injunctive claims can be the most important part of a class action).

277. *See* Moore v. Apple Inc., 309 F.R.D. 532, 541 (N.D. Cal. 2015) ("In sum, the Court finds that Plaintiff has satisfied the standing requirements under Article III.").

278. *See* Backhaut v. Apple Inc., No. 14–CV–02285–LHK, 2015 WL 4776427,

their attempt to certify an injunctive class because they could not prove a threat of future injury,[279] the plaintiffs in *Moore* obtained internal Apple documents through discovery that proved Apple was aware that "hundreds of former iPhone users reported attempting deactivation but were still not receiving text messages from Apple device users."[280] And while the *Moore* case turned on the issue of reading every single proposed class member's contract to determine whether there had indeed been a "harm," the harm question under a conversion or trespass to chattels theory would be much simpler: Did the proposed class members fail to receive text messages they were supposed to?[281] Yes.[282] Therefore, the plaintiffs would have probably succeeded in certifying an injunctive class because the plaintiffs could use Apple's knowledge of the problem to prove both present harm and future harm.[283]

That is why, if iMessage plaintiffs brought either trespass to chattels or conversion claims against Apple for Apple's disrupting their text message delivery, and if the court agreed that text messages constitute intangible personal property, the result would have been different. The plaintiffs would have certified their Rule

---

at *8 (N.D. Cal. Aug. 13, 2015) (outlining the requirements necessary "to establish standing for injunctive relief").

279. *See id.* at *8–9 (explaining how each of the *Backhaut* plaintiffs have either started using iPhones again or begun receiving text messages from current iPhone users, indicating that there was no risk of future harm).

280. *See Moore*, 309 F.R.D. at 537 (reviewing internal documents "apparently discussing how Apple's 'so-called fixes' failed to address the disruptions in text message delivery").

281. *See In re* Apple & ATTM Antitrust Litig., No. C 07–05152 JW, 2010 WL 3521965, at *13 (N.D. Cal. July 8, 2010), *vacated in part*, 826 F. Supp. 2d 1168 (2011) (explaining that certifying an injunctive class is appropriate if the plaintiffs prove that, should they succeed on the merits, injunctive relief would be "reasonably necessary and appropriate").

282. *See Moore*, 73 F. Supp. 3d at 1196 ("Plaintiff is not the only former Apple device user to encounter the problem of undelivered text messages. '[C]ountless' former Apple device users have not received messages sent by Apple device users.").

283. *See Moore*, 309 F.D.R. at 542 (denying class certification because the plaintiff's proposed class included "individuals who did not pay or contract for text messaging services," and were thus not harmed by Apple's withholding their text messages).

23(b)(2) injunctive class.[284] Apple would have then been forced to begin delivering text messages sent to former iMessage users. And current iPhone owners might even feel comfortable leaving Apple's "walled garden" ecosystem to try out a competitor's cellular device without fear that Apple will "lose" text messages meant for them.[285]

C. Why the Third-Party Loophole Will Begin to Close

Recall that the third-party loophole is the exception that enables the government to obtain consumer information from companies without a search warrant.[286] Although the Fourth Amendment bars the government from searching the contents of your cell phone without a warrant, the Constitution does not bar the government from searching the same exact information when it is stored on the cloud instead of your cell phone.[287] While courts have begun closing the third-party loophole as it pertains to e-mails sent through and stored with internet service providers (ISPs), courts have not shown the same willingness to protect text messages stored on the cloud and sent through wireless service providers.[288]

Classifying text messages as property closes the third-party loophole for two reasons. First, text message owners manifest their

---

284. *See In re Apple & ATTM Antitrust Litig.*, 2010 WL 3521965, at *14 (certifying the proposed injunctive class because the plaintiffs proved that "injunctive relief from the challenged conduct would be reasonably necessary and appropriate if Plaintiffs succeed on the merits").

285. *See supra* notes 132–137 and accompanying text (describing iPhone users who feel locked in to their device and unable to switch to another type of cell phone because of iMessage).

286. *Supra* Part II.B.

287. *See* Riley v. California, 573 U.S. 373, 401–03 (2014) (extending constitutional "probable cause" protection to information stored within a cell phone).

288. *See* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."); Warshak v. United States, 631 F.3d 266, 288 (6th Cir. 2010) (holding that because "a subscriber enjoys a reasonable expectation of privacy in the contents of emails" sent or stored with ISPs, "[t]he government may not compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause").

intent to prevent third parties and the government from reading the content of their encrypted property.[289] This "intent to prevent" is at odds with the third-party doctrine's theory that an individual who voluntarily conveys information to a third party has no reasonable expectation of privacy.[290]

Extending personal property protections to text messages introduces a different legal theory relevant to determining whether the text messages can be searched without a warrant: the "container doctrine."[291] Under the container doctrine, courts give seemingly-abandoned personal property contained within a secure container greater constitutional protections against warrantless searches because the act of securing personal property shows the owner's express manifest intent to keep the property protected.[292] Text messages, an intangible personal property, are placed outside of their owner's control when they are stored on the cloud.[293] And

289. *See* David Kravets, *Here's A Good Reason to Encrypt Your Data*, WIRED (Apr. 23, 2013, 6:29 PM), https://www.wired.com/2013/04/encrypt-your-data/ (last visited Mar. 19, 2019) (explaining that a "top reason" to encrypt data "is to keep the government out of your hard drive") (on file with the Washington and Lee Law Review).

290. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (finding that one has no expectation of privacy in information handed over to third parties).

291. *See* FAIRFIELD, *supra* note 211, at 127 ("[O]utside of the owner's possession or control, the property can be considered abandoned, at least for privacy purposes, and thus can be searched. This is the abandonment doctrine. On the other hand, property placed inside containers has historically been given much stronger protection from searches and seizures.").

292. *See* United States v. Chadwick, 433 U.S. 1, 10 (1977)

> By placing personal effects inside a double-locked footlocker, respondents manifested an expectation that the contents would remain free from public examination. No less than one who locks the doors of his home against intruders, one who safeguards his personal possessions in this manner is due the protection of the Fourth Amendment Warrant Clause. There being no exigency, it was unreasonable for the Government to conduct this search without the safeguards a judicial warrant provides.

293. *See* FAIRFIELD, *supra* note 211, at 128 (explaining how "[t]he very purpose of [digital] assets is that they are [stored] away from their owners but not out of their owners' control").

remember that Apple stores copies of all iMessage and SMS communications on the cloud.[294] AT&T and Verizon do too.[295]

The classic example of property receiving greater protections against warrantless searches is a padlocked box, whose owner manifested an intent to keep the property protected by locking the box.[296] By analogy, a text message owner should receive heightened protections against warrantless searches because the owner, by "locking" the contents of the text message with encryption technology, has manifested an intent to keep the property protected, even if Apple stores a copy of the text message on an iCloud server outside the possession of its owner.

Text message users rely on iMessage's end-to-end encryption to keep their text messages secure both in the cloud and in transit.[297] Also, most text message users rely on their smartphone's lock screen to keep unwanted intruders out of their text message inbox.[298] Encryption, coupled with smartphone security features, serve as the text message user's manifest intent and expectation that their text messages be secure against unwanted intrusions.

---

294. *See Privacy*, *supra* note 237 ("iMessage and SMS messages are backed up on iCloud for your convenience, but you can turn iCloud Backup off whenever you want.") (on file with the Washington and Lee Law Review).

295. *See AT&T Privacy Policy*, AT&T, http://about.att.com/sites/privacy_policy/terms#collect (last visited Mar. 19, 2019) ("We may collect different types of information based on your use of our products and services and on our business relationship with you. Examples of this might include . . . the number of text messages sent and received . . . [and] calling and texting records.") (on file with the Washington and Lee Law Review); *Privacy Policy*, VERIZON (Jan. 2018), http://www.verizon.com/about/privacy/full-privacy-policy (last updated April 2018) (last visited Mar. 19, 2019) ("We collect information when you communicate with us and when you use our products, services and sites.") (on file with the Washington and Lee Law Review).

296. *See Chadwick*, 433 U.S. at 10 ("By placing personal effects inside a double-locked footlocker, respondents manifested an expectation that the contents would remain free from public examination.").

297. *See About iMessage and SMS/MMS*, APPLE (Sept. 17, 2018), https://support.apple.com/en-us/HT207006 (last visited Jan. 28, 2019) (explaining the security differences between iMessages and SMS text messages) (on file with the Washington and Lee Law Review).

298. *See Americans and Cybersecurity*, PEW RES. CTR. (Jan. 26, 2017), http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/ (last visited Mar. 19, 2019) (outlining how 72% of smartphone users "use a screen lock or other security features" to secure their devices) (on file with the Washington and Lee Law Review).

A text message owner's plainly evident intent to prevent unwanted intrusions during transit and storage does not square with the third-party doctrine's legal fiction that the same text message owner has no reasonable expectation of privacy if she sends her text message through a cellular service provider. The opposite is true. A text message owner's intent to prevent unwanted intrusions into her text message property *proves* her reasonable expectation of privacy.[299] Consequently, as the text message owner retains her reasonable expectation of privacy with regard to the text message's content during transit and storage, the third-party loophole closes because the government cannot collect information which has not been disclosed to the third party.

Second, text messages, as a form of property and not merely confidential information, are encrypted to prevent third parties from viewing the text message's content.[300] Instead of traveling through cyberspace as an open book, the encrypted text message travels under lock and key, and thus the content within is at no point conveyed to the cellular service provider.[301] Because a third-party service provider never sees the content hidden by encryption, the text message's content is never revealed to the service provider.

If the content remains hidden behind encryption, then the text message user has not voluntarily conveyed the content to the provider because the provider does not see the content.[302] As well, the service provider cannot claim it saw the text message's content confidentially because it never saw the content at all.[303] Cellular

---

299. *See* Warshak v. United States, 631 F.3d 266, 288 (6th Cir. 2010) (explaining that the government may not collect e-mails under the third-party doctrine because the e-mail users retained their reasonable expectation of privacy).

300. *See* Kopfstein, *infra* note 304 (explaining why Apple encrypts iMessages).

301. *See id.* (describing iMessage's end-to-end encryption and how it (in theory) means that only the sender and the recipient will read the message's content).

302. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

303. *See* United States v. McIntyre, 646 F.3d 1107, 1112 (8th Cir. 2011) (finding that one's expectation of confidentiality with regard to information shared with third parties has no bearing on the information's Fourth Amendment

service providers are not meant to read any of the text message's content—even if they do anyway—by virtue of the text message remaining sealed (encrypted) in transit and during storage.[304] So, because a text message owner does not convey the content of the text message to the cellular service provider, confidentially or otherwise, the government cannot get the text message's content using the third-party loophole.[305]

Just as the government cannot open up a sealed letter and read its contents without a warrant, the government should be prevented from opening up encrypted text messages, whether stored or in transit, without a warrant.[306] Although the framers had sealed letters in mind when adopting the Fourth Amendment, there is hardly a more appropriate modern analogy than an encrypted text message.[307]

VI. Conclusion

Courts have yet to consider whether text messages constitute intangible personal property, but they will soon. As our lives

---

protections).

304. *See* Janus Kopfstein, *Apple Can Still See Your iMessages If You Enable iCloud*, VICE (Jan. 22, 2016, 4:10 PM), https://motherboard.vice.com/en_us/article/78kv7b/psa-apple-can-still-see-your-imessages-if-you-enable-icloud (last visited Mar. 19, 2019)

> It turns out the privacy benefits Apple likes to talk about (and the FBI likes to complain about) basically disappear when iCloud Backup is enabled. Your messages, photos and whatnot are still protected while on your device and encrypted end-to-end while in transit. But you're also telling your device to CC Apple on everything. Those copies are encrypted on iCloud using a key controlled by Apple, not you, allowing the company (and thus anyone who gets access to your account) to see their contents.

(on file with the Washington and Lee Law Review).

305. *See id.* ("Apple can't read messages sent between Apple devices because they're encrypted end-to-end, decipherable only by you and the intended recipient.").

306. *See* United States v. Ackerman, 831 F.3d 1292, 1308 (10th Cir. 2016) ("[T]he framers were concerned with the protection of physical rather than virtual correspondence. But a more obvious analogy from principle to new technology is hard to imagine and, indeed, many courts have already applied the common law's ancient trespass to chattels doctrine to electronic, not just written, communications.").

307. *Id.*

become more and more centered around our smartphones, text messages will displace e-mails as the primary means of electronic communication (if that hasn't already happened). We currently do not have an effective means of recourse available should our cellular providers purposefully block or delete our text messages.

The answer lies in property law. Text messages constitute intangible personal property, and text message owners can, therefore, sue using traditional property law causes of action such as trespass to chattels or conversion. Although there have been few legal challenges brought by aggrieved text message owners, they have been universally unsuccessful in causing cellular providers to change their ways.[308] Had these aggrieved text message owners sued under a property-based cause of action, they would have successfully enjoined the cellular providers from continuing to mess with their text messages.

Moreover, a judicial determination that text messages constitute intangible personal property will close the third-party loophole. As it stands, the government is free to search the contents of our text messages because we have voluntarily conveyed the information to our cellular service providers.[309] However, if courts find that text messages constitute a form of property, an encrypted text message starts to look more and more like a sealed letter than it does public information. The framers designed the Fourth Amendment to prevent unwarranted searches and seizures of the dominant form of communication of their day: sealed letters. Consequently, it makes sense to extend the Fourth Amendment's protection only to the dominant form of communication today: encrypted text messages.

308. *Supra* Part IV.A.

309. *Supra* Part IV.B.