THE THIRD-PARTY DOCTRINE: PERPETUATION BY PRIVACY POLICIES

COURTNEY C. SEITZ*

INTRODUCTION

"When you use Uber, you trust us with your information. We are committed to keeping that trust. That starts with helping you understand our privacy practices."[1]

With the check of a box or the click of a button, consumers and users consent to privacy policies and entrust their personal information to countless companies and service providers.[2] For example, when a user agrees to Uber's privacy policy, he or she permits Uber to "collect and use personal information to provide [its] services."[3] Such personal information "may include your name, email, phone number, login name and password, address, payment or banking information (including related payment verification information), government identification numbers such as Social Security number, driver's license or passport if required by law, birth date, photo and signature."[4] Not only is a user sharing his or her personal information with Uber, but he or she is also potentially consenting to the transfer of such information to third parties.[5] Many

* Candidate for Juris Doctor, Notre Dame Law School, 2020; Bachelor of Science in Accounting and Marketing with a Minor in Philosophy, Boston College, 2014. I would like to thank Dean Randy Kozel for his guidance and thoughtful feedback throughout this writing process. I would like to thank my parents and my sister for their love, encouragement, and support. All errors are my own.

1. *Privacy Policy*, UBER, https://privacy.uber.com/policy (last updated May 25, 2018); *see also Data Policy*, FACEBOOK, https://www.facebook.com/privacy/explanation (last updated Apr. 19, 2018) ("This policy describes the information we process to support Facebook, Instagram, Messenger and other products and features offered by Facebook . . . .").

2. *See, e.g.*, FACEBOOK, https://www.facebook.com (last visited May 22, 2019) ("By clicking Sign Up, you agree to our Terms, Data Policy and Cookies Policy."); UBER, https://auth.uber.com/login/?uber_client_name=riderSignUp& (last visited May 22, 2019) ("By clicking 'Sign Up', you agree to Uber's Terms of Use and acknowledge you have read the Privacy Policy.").

3. *Privacy Policy*, *supra* note 1.

4. *Id.*

5. *See, e.g.*, *id.* ("Uber may provide information to its vendors, consultants, marketing partners, research firms, and other service providers or business partners."); *id.* ("Uber may share your information if we believe it is required by applicable law, regulation, operating agreement, legal process or governmental request, or where the disclosure is otherwise appropriate due to safety or similar concerns.").

consumers and users agree to such privacy policies without even reading the fine print that impacts their privacy rights.[6] When a user accepts such terms, the company generally has the right to collect, use, and share such information. Does a user's acceptance of a privacy policy mean that he or she forfeits his or her Fourth Amendment rights in such information?

The Fourth Amendment protects an individual "against unreasonable searches and seizures" by the government.[7] The "essence of [a Fourth Amendment] offence . . . is the invasion of [a person's] indefeasible right to personal security, personal liberty and private property . . . ."[8] This amendment has been construed to provide "a powerful protection of one's papers and personal information."[9] However, when an individual seeks to protect information provided to others, the third-party doctrine rears its head. This doctrine holds "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[10] Thus, when a consumer or user agrees to a company's or service provider's privacy policy, he or she potentially forfeits Fourth Amendment protection of his or her personal data. In tandem with privacy policies, does the third-party doctrine represent a legal loophole through which Fourth Amendment privacy protections are sacrificed?

This Note evaluates the interplay between the third-party doctrine and privacy policies. Specifically, it argues that privacy policies perpetuate the third-party doctrine. Part I examines the constitutional context of the third-party doctrine, defines the third-party doctrine, and explores its development through three cases: *Katz v. United States*,[11] *United States v. Miller*,[12] and *Smith v. Maryland*.[13] Part II evaluates the Supreme Court's 5-4 decision in *Carpenter v. United States*.[14] There, the majority did not overturn the third-party doctrine but "decline[d] to extend" it.[15] As such, the third-party doctrine is still good law. Turning to privacy policies, Part III provides a brief background on them. It focuses on defining privacy policies, the United States' sectoral approach to

---

6. *See* Joel R. Reidenberg et al., *Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding*, 30 BERKELEY TECH. L.J. 39, 41 (2015) [hereinafter Reidenberg et al., *Disagreeable Privacy Policies*] ("Privacy policies are verbose, difficult to understand, take too long to read, and may be the least-read items on most websites even as users express growing concerns about information collection practices.").

7. U.S. CONST. amend. IV.

8. Daniel J. Solove, *A Brief History of Information Privacy Law* 8–9 (George Washington Univ. Law Sch. Pub. Law, Research Paper No. 215, 2016) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)), https://ssrn.com/abstract=914271 (describing *Boyd*'s impact on Fourth Amendment jurisprudence).

9. *Id.* at 9.

10. Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018) (quoting Smith v. Maryland, 442 U.S. 735, 743–44 (1979)).

11. Katz v. United States, 389 U.S. 347 (1967).

12. United States v. Miller, 425 U.S. 435 (1976).

13. Smith v. Maryland, 442 U.S. 735 (1979).

14. *Carpenter*, 138 S. Ct. 2206.

15. *Id.* at 2220.

privacy law regulation, and the Federal Trade Commission's role. Finally, Part IV analyzes how privacy policies enable the continued application of the third-party doctrine in a post-*Carpenter* era. However, it recognizes the third-party doctrine will likely persist in an altered form and contemplates its reformulation.

I. THE THIRD-PARTY DOCTRINE: DISTINGUISHED, DEFINED, AND DELINEATED

A. The Fourth Amendment

The Fourth Amendment to the United States Constitution holds:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[16]

The purpose of this amendment is to "protect[] people."[17] Its protective function is activated when (1) "a person ha[s] exhibited an actual (subjective) expectation of privacy" and (2) "the expectation [is] one that society is prepared to recognize as 'reasonable.'"[18] When each of these requirements is met an "official intrusion into [a] private sphere generally qualifies as a search and requires a warrant supported by probable cause."[19] Probable cause exists when "there is a fair probability that contraband or evidence of a crime will be found in a particular place."[20]

B. The Third-Party Doctrine

The third-party doctrine holds that an individual "has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[21] It has two key components: (1) a "legitimate expectation of privacy" and (2) voluntary disclosure. A "legitimate expectation of privacy" is "one that society is prepared to recognize as reasonable."[22] The concept of voluntary disclosure contemplates that when a person willingly shares information with others, he or she assumes the risk that such data could be further distributed.[23] Society has not yet recognized a person's privacy interest in information

16. U.S. CONST. amend. IV.

17. Katz v. United States, 389 U.S. 347, 351 (1967).

18. *Id.* at 361 (Harlan, J., concurring).

19. *Carpenter*, 138 S. Ct. at 2213.

20. Illinois v. Gates, 462 U.S. 213, 238 (1983).

21. *Carpenter*, 138 S. Ct. at 2216 (quoting Smith v. Maryland, 442 U.S. 735, 743–44 (1979)).

22. *Id.* (quoting *Smith*, 442 U.S. at 743).

23. *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.").

voluntarily disclosed to third parties.[24] When a person does share information with others, it does not receive Fourth Amendment protection and its use is governed by the third-party doctrine.[25] From a procedural perspective, the absence of Fourth Amendment protection means that government actors can access a citizen's personal information or data without a warrant (i.e., lowering the evidentiary standard from probable cause).[26] Thus, this doctrine reduces a person's privacy rights with respect to information shared with third parties.

The following subsections examine the contributions of three cases to the third-party doctrine: *Katz v. United States*,[27] *United States v. Miller*,[28] and *Smith v. Maryland*.[29]

1. *Katz v. United States*

Convicted for contravening a federal statute by "transmitting wagering information by telephone from Los Angeles to Miami and Boston," the *Katz* petitioner claimed that his Fourth Amendment rights were violated when the government presented incriminating evidence obtained by recording his conversations in a "public telephone booth."[30] As "[t]here was no physical entrance [by the government] into the area occupied by, [the petitioner]," the lower courts did not find a Fourth Amendment violation.[31] However, the Supreme Court's majority took a different approach.

Contrary to the lower courts, the Supreme Court held that the petitioner's Fourth Amendment rights were violated by the government's electronic surveillance.[32] By "electronically listening to and recording the petitioner's words [the government] violated the privacy upon which he justifiably relied while using the telephone booth and thus [the government's actions] constituted a 'search and seizure' within the meaning of the Fourth Amendment."[33] Recognizing that "the Fourth Amendment protects people, not places," the Court explained "what [a person] seeks to preserve as private, even in an area

24. *See Carpenter*, 138 S. Ct. at 2216 ("[T]he Court has drawn a line between what a person keeps to himself and what he shares with others.").

25. *See Miller*, 425 U.S. at 443 ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.").

26. *See Carpenter*, 138 S. Ct. at 2216 ("[T]he Government is typically free to obtain [voluntarily shared] information from the recipient without triggering Fourth Amendment protections.").

27. Katz v. United States, 389 U.S. 347 (1967).

28. *Miller*, 425 U.S. 435.

29. Smith v. Maryland, 442 U.S. 735 (1979).

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

31. *Id.* at 348–49 (alterations in original) (quoting Katz v. United States, 369 F.2d 130, 134 (9th Cir. 1966)).

32. *Id.* at 353.

33. *Id.*

accessible to the public, may be constitutionally protected."[34] Adding fuel to the fire, the government failed to follow the constitutionally approved practice of obtaining a warrant prior to carrying out its investigation.[35]

While the majority's opinion is notable for its recognition of the potential for constitutionally protected privacy in public places, the case's key contribution to the third-party doctrine comes from Justice Harlan's concurrence. In agreeing with the majority, Justice Harlan delineated a two-part test for Fourth Amendment privacy protection. First, "a person [must] have exhibited an actual (subjective) expectation of privacy."[36] Second, a person's "expectation [must] be one that society is prepared to recognize as 'reasonable.'"[37] Applying this test to the case at hand, Justice Harlan honed in on the fact that a telephone booth user expects privacy when making a call.[38] The telephone booth user's expectations of privacy were warranted because society confirmed them.[39] Thus, when the government intruded on the petitioner's societally recognized expectation of privacy, his Fourth Amendment rights were violated.

Although Justice Harlan's two-part test pertains to the Fourth Amendment, it also helps to define a paramount phrase in the third-party doctrine: "legitimate 'expectation of privacy.'"[40] An expectation that is legitimate is an expectation "that society is prepared to recognize as 'reasonable.'"[41]

2. *United States v. Miller*

Justice Harlan's language resurfaced in *Miller* almost ten years later. In that case, the respondent asserted that his Fourth Amendment rights were violated when "copies of checks and other bank records [were] obtained by means of allegedly defective subpoenas *duces tecum* served upon two banks at which he had accounts."[42] He claimed that "he ha[d] a reasonable expectation

---

34. *Id.* at 351.

35. *See id.* at 357. "'Over and again this Court has emphasized that the mandate of the [Fourth] Amendment requires adherence to judicial processes' and that searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment . . . ." *Id.* (alteration in original) (citation omitted) (quoting United States v. Jeffers, 342 U.S. 48, 51 (1951)).

36. *Id.* at 361 (Harlan, J., concurring).

37. *Id.*

38. *Id.* "The critical fact in this case is that '[o]ne who occupies it, [a telephone booth] shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume' that his conversation is not being intercepted." *Id.* (alterations in original) (quoting *id.* at 352 (majority opinion)).

39. *Id.* "The point is not that the booth is 'accessible to the public' at other times but that it is a temporarily private place whose momentary occupants' expectations of freedom from intrusion are recognized as reasonable." *Id.* (citation omitted) (quoting *id.* at 351 (majority opinion)).

40. United States v. Miller, 425 U.S. 435, 442 (1976).

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

42. *Miller*, 425 U.S. at 436.

of privacy" in the information shared and that the materials "were made available to the banks for a limited purpose."[43] The Court disagreed. It emphasized that the records were not the respondent's, but that of third parties.[44] Ultimately, it held "that respondent had no protectable Fourth Amendment interest in the subpoenaed documents."[45]

In striking down the respondent's Fourth Amendment claim, the Court executed a third-party doctrine analysis. First, it explained the respondent had "no legitimate 'expectation of privacy' in [the] contents" of the documents shared with the bank.[46] The Court highlighted that "[t]he checks are not confidential communications but negotiable instruments to be used in commercial transactions."[47] The Court bolstered this point with a legislative history argument. It explained that "[t]he lack of any legitimate expectation of privacy concerning the information kept in bank records was assumed by Congress in enacting the Bank Secrecy Act" in order to support government investigations.[48] As such, it was unreasonable for the respondent to expect a privacy interest in the disputed documents.

Second, the Court explained that the documents "contain[ed] only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[49] When he "reveal[s] his affairs to another," "[t]he depositor takes the risk . . . that the information will be conveyed by that person to the Government."[50] Thus, by voluntarily sharing his information with the bank, the respondent assumed the risk that the checks would be shared with other parties.

Because the respondent had no legitimate expectation of privacy in the "business records" or "negotiable instruments" voluntarily shared with the banks, his Fourth Amendment claim fell prey to the third-party doctrine.[51]

3. *Smith v. Maryland*

In *Smith*, the Court considered "whether the installation and use of a pen register[52] constitutes a 'search' within the meaning of the Fourth Amendment."[53] The petitioner claimed his Fourth Amendment rights were

43. *Id.* at 442.

44. *Id.* at 440 ("On their face, the documents subpoenaed here are not respondent's 'private papers.' . . . Instead, these are the business records of the banks.").

45. *Id.* at 437.

46. *Id.* at 442.

47. *Id.*

48. *Id.* at 442–43.

49. *Id.* at 442.

50. *Id.* at 443.

51. *Id.* at 440–42.

52. By definition, a pen register is "a device that registers the numbers dialed from a telephone." *Pen Register*, MERRIAM-WEBSTER, https://www.merriam-webster.com/legal/pen%20register (last visited Feb. 7, 2019).

53. Smith v. Maryland, 442 U.S. 735, 736 (1979) (footnote omitted).

violated when the police, without warrant, installed a pen register "to record the numbers dialed from [his] telephone."[54] He contended "that he had a 'legitimate expectation of privacy' regarding the numbers he dialed on his phone."[55] Based on Justice Harlan's two-part Fourth Amendment test and a third-party doctrine analysis, the Court rebuked his claim.

The Court started with Justice Harlan's test as described in *Katz*.[56] First, the Court found it highly unlikely that the petitioner had an "actual expectation of privacy in the phone numbers he dialed."[57] Taking a common-sense approach, the Court explained "[t]elephone users . . . typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes."[58] Second, the Court noted that had the petitioner truly exhibited a belief that he was privately punching numbers into his telephone, such a belief was illegitimate.[59] The Court commented it has "consistently . . . held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[60]

Having already determined that the petitioner lacked a "legitimate expectation of privacy" in telephone numbers, the Court focused on his voluntary disclosure of information. Likening the petitioner's situation to that of the respondent in *Miller*, the Court explained "[w]hen he used his phone, petitioner voluntarily conveyed numerical information to the telephone company."[61] The "petitioner assumed the risk that the company would reveal to police the numbers he dialed."[62]

The above analyses compelled the Court to "conclude that [the] petitioner . . . entertained no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, his expectation was not 'legitimate.'"[63] Therefore, it held the police's pen register installation was not a warrantless search that violated the petitioner's Fourth Amendment rights.[64] The third-party doctrine prevailed.

---

54. *Id.* at 737.

55. *Id.* at 742.

56. See *id.* at 739–44.

57. *Id.* at 745.

58. *Id.* at 743.

59. *Id.* at 745. "Second, even if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not 'one that society is prepared to recognize as "reasonable."'" *Id.* at 743 (quoting Katz v. United States, 389 U.S. 347, 361 (1967)).

60. *Id.* at 743–44.

61. *Id.* at 744.

62. *Id.*

63. *Id.* at 745.

64. *Id.* at 745–46.

II. *CARPENTER V. UNITED STATES*

Decades after its initial development, the third-party doctrine still stands. In 2018, *Carpenter v. United States* appeared to be a case ripe for the application of the third-party doctrine. In the 5-4 decision, the majority did not apply the third-party doctrine.[65] However, it "d[id] not disturb the application of *Smith* and *Miller*."[66] Ultimately, and seemingly uncharacteristically, the Court upheld the petitioner's Fourth Amendment rights.[67] While it did not touch the third-party doctrine, the Court's privacy-protective ruling leaves open questions as to the future of the third-party doctrine in our technological times.[68] The following section analyzes the Court's rationale for evading the third-party doctrine and the four dissenters' divergent approach.[69]

A. The Majority

Carpenter, like the above-mentioned cases, also involved a Fourth Amendment claim. The petitioner "argued that the Government's seizure of the [cell-site location information (CSLI)] records violated the Fourth Amendment because they had been obtained without a warrant supported by probable cause."[70] Pursuant to the Stored Communications Act, the government used "court orders" to obtain the petitioner's information from his cell phone providers: MetroPCS and Sprint.[71] As opposed to probable cause, the Stored Communications Act requires a lesser evidentiary standard to obtain information; it only requires a demonstration of "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[72] Thus, the petitioner claimed his Fourth Amendment rights were violated.

---

65. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

66. *Id.*

67. *Id.* ("[T]he fact that the Government obtained the information from a third party d[id] not overcome Carpenter's claim to Fourth Amendment protection. The Government's acquisition of the cell-site records was a search within the meaning of the Fourth Amendment.").

68. While *Carpenter* did not overturn the third-party doctrine, many have touted the decision as a win for privacy rights. *See, e.g.*, Michael Price, Carpenter v. United States *and the Future Fourth Amendment*, CHAMPION, June 2018, at 48 ("[*Carpenter*] has set a course for rethinking Fourth Amendment rights in the digital age. It is the third bright star in the last seven years, marking a welcome and long overdue departure from the so-called 'third-party doctrine' that has limited privacy rights for the last four decades.").

69. It is worth noting that the Court of Appeals for the Sixth Circuit applied the third-party doctrine. It "held that Carpenter lacked a reasonable expectation of privacy in the location information collected by the FBI because he had shared that information with his wireless carriers" and because "cell phone users voluntarily convey cell-site data to their carriers . . . the resulting business records are not entitled to Fourth Amendment protection." *Carpenter*, 138 S. Ct. at 2213.

70. *Id.* at 2212.

71. *Id.*

72. 18 U.S.C. § 2703(d) (2018); *see also Carpenter*, 138 S. Ct. at 2212.

The Court was left to decide "whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements."[73] Based on its prior decisions, one might argue that the Court could apply the third-party doctrine analysis, determine that the petitioner lacked a legitimate privacy expectation in the information, discern that the information was willingly shared with a third party, and deny the petitioner's Fourth Amendment claim. However, that was not the case in *Carpenter*. The Court explained that it could analyze this question under one of two approaches: (1) it could consider whether a person has an "expectation of privacy in his physical location and movements" or (2) it could consider whether information was shared with a third party in which case an individual would have "no legitimate expectation of privacy."[74] The Court explained, "[g]iven the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection."[75] Thus, the Court decided to move forward with the former mode of analysis.

Pointing to precedent, the Court proceeded to apply the principles set forth in *United States v. Knotts*[76] and *United States v. Jones*.[77] Both of these cases focus on a person's physical location and movements.[78] In *Knotts*, the Court considered whether the "use of a beeper [to keep tabs on a motor vehicle's travels] violated [the] respondent's rights secured by the Fourth Amendment to the United States Constitution."[79] The Court held that such surveillance did not violate the respondent's constitutional rights because "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[80] In *Jones*, however, the Court changed its tune. There, similar to *Knotts*, it examined "whether the attachment of a Global-Positioning-System (GPS) tracking device to an individual's vehicle, and subsequent use of that device to monitor the vehicle's movements on public streets, constitutes a search or seizure within the meaning of the Fourth Amendment."[81] Unlike *Knotts*, however, the Court found a Fourth Amendment violation. The Court explained: "[t]he Government physically occupied private property for the purpose of obtaining information" and "such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted."[82] Thus, it held "the

73. *Carpenter*, 138 S. Ct. at 2211.

74. *Id.* at 2215–16 (quoting Smith v. Maryland, 442 U.S. 735, 743–44 (1979)).

75. *Id.* at 2217. Justice Gorsuch partially echoes this sentiment in his dissent. *See id.* at 2270 (Gorsuch, J., dissenting) ("[J]ust because you *have* to entrust a third party with your data doesn't necessarily mean you should lose all Fourth Amendment protections in it.").

76. United States v. Knotts, 460 U.S. 276 (1983).

77. United States v. Jones, 565 U.S. 400 (2012).

78. *See Knotts*, 460 U.S. 276; *Jones*, 565 U.S. 400.

79. *Knotts*, 460 U.S. at 277.

80. *Id.* at 281.

81. *Jones*, 565 U.S. at 402.

82. *Id.* at 404–05.

Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.'"[83] Essentially, these two cases consider a person's privacy interest in his or her "physical movements."[84]

In applying *Knotts* and *Jones* to *Carpenter*, the Court focused on the character of the information that the government collected.[85] The government collected the petitioner's cell-site location information which enabled it to "chronicle [the petitioner's] past movements through the record of his cell phone signals."[86] The Court explained that "historical cell-site records present even greater privacy concerns than the GPS monitoring of a vehicle . . . considered in *Jones*."[87] Because people "compulsively carry cell phones with them all the time," the government was able to obtain unprecedented access to the petitioner's location.[88] As such, the Court held that "[t]he Government's acquisition of the cell-site records was a search within the meaning of the Fourth Amendment."[89] Since the government's actions constituted a search, it was required to secure a warrant.[90] The "court order issued under the Stored Communications Act" was insufficient.[91]

Though the Court did not apply the third-party doctrine in this context, the Court did explain why the third-party doctrine did not apply. First, the Court discussed the third-party doctrine's "legitimate expectation of privacy" prong.[92] The Court distinguished *Miller* and *Smith* from *Carpenter* based on the character of the items at issue. Whereas the "pen register" in *Smith* had "limited capabilities" and the business records in *Miller* were "negotiable instruments" such that privacy interests could not be claimed, Carpenter's CSLI represented "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years."[93] The Court identified "[s]uch a chronicle implicates privacy concerns far beyond those considered in *Smith* and *Miller*."[94] Second, it keyed in on the lack of voluntariness associated with the disclosure of CSLI. The Court identified a cell phone as "indispensable to participation in modern society."[95] It explained "a cell phone logs a cell-site record by dint of

83. *Id.* at 404 (footnote omitted).

84. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

85. *Id.* at 2214 ("The case before us involves the Government's acquisition of wireless carrier cell-site records revealing the location of Carpenter's cell phone whenever it made or received calls.").

86. *Id.* at 2216.

87. *Id.* at 2218.

88. *Id.*

89. *Id.* at 2220.

90. *Id.* at 2221.

91. *Id.*

92. *Id.* at 2217.

93. *Id.* at 2219–20.

94. *Id.* at 2220.

95. *Id.*

its operation, without any affirmative act on the part of the user" such that "in no meaningful sense does the user voluntarily . . . turn[] over a comprehensive dossier of his physical movements."[96]

Ultimately, the majority stressed the "narrow" nature of its holding.[97] It cited Justice Frankfurter who "noted when considering new innovations in airplanes and radios, the Court must tread carefully in such cases, to ensure that [it] do[es] not 'embarrass the future.'"[98] While it "tread carefully," the majority's privacy-protective stance identified the need for change. The Court seemingly strategically analyzed the question presented under the *Knotts* and *Jones* precedents, as opposed to the *Smith* and *Miller* framework, to broaden individuals' privacy protections amidst technological times. Had the Court conducted a traditional third-party doctrine analysis of *Carpenter* it could have potentially found no protectable Fourth Amendment interest in the CSLI. As it is "narrow" and did not nullify the third-party doctrine, *Carpenter's* holding leaves open questions for the future of privacy rights.

B. The Dissents

While the majority's opinion signals a privacy-protective approach, a property-centric defense of the Fourth Amendment reverberates through the dissents. The following section analyzes each dissent in turn.

Leading the charge, Justice Kennedy maintained the "case should be resolved by interpreting accepted property principles as the baseline for reasonable expectations of privacy."[99] In deciding "the Government did not search anything over which Carpenter could assert ownership or control," Justice Kennedy cited Fourth Amendment property ideals and the *Miller* and *Smith* line of cases.[100] He explained that the Fourth Amendment "protects only a person's own 'persons, houses, papers, and effects.'"[101] *Miller* and *Smith* reinforce this concept by "limit[ing] . . . the ability of individuals to assert Fourth Amendment interests in property to which they lack a 'requisite connection.'"[102] Like the documents at issue in *Miller* and *Smith*, the CSLI at issue in *Carpenter* was "created, kept, classified, owned, and controlled by cell phone service providers."[103] Justice Kennedy emphasized that "[c]ustomers do not create the records" and explained "[b]ecause Carpenter lacks a requisite connection to the cell-site records, he also may not claim a reasonable expectation of privacy in them."[104] Thus, per the call of the constitutional

96. *Id.*
97. *Id.*
98. *Id.* (quoting Nw. Airlines, Inc. v. Minnesota, 322 U.S. 292, 300 (1944)).
99. *Id.* at 2235 (Kennedy, J., dissenting).
100. *Id.*
101. *Id.* at 2227.
102. *Id.* (quoting Minnesota v. Carter, 525 U.S. 83, 99 (1998) (Kennedy, J., concurring)).
103. *Id.* at 2229.
104. *Id.* at 2229–30.

provision, Carpenter should not have been afforded Fourth Amendment protections in records that were not his own property.

In Justice Thomas's view, the determinative question was "*whose* property was searched."[105] He stated simply: "The records [at issue] belong to MetroPCS and Sprint."[106] Under a traditional and textual understanding of the Fourth Amendment, Carpenter would be unable to assert Fourth Amendment rights in another party's records. However, under the majority's application of *Katz's* "'reasonable expectation of privacy' test," it found a Fourth Amendment violation.[107] Thus, Justice Thomas dissented to express his discontent with the *Katz* test.[108]

According to Justice Thomas, "[t]he *Katz* test has no basis in the text or history of the Fourth Amendment."[109] He turned to the text of the Fourth Amendment itself to prove this contention. For example, he singled out the word "their."[110] This word "means, at the very least, that individuals do not have Fourth Amendment rights in *someone else's* property."[111] However, "under the *Katz* test, individuals can have a reasonable expectation of privacy in another person's property."[112] Therefore, Justice Thomas claimed "the Founders would be puzzled by the Court's conclusion" and challenged the Court to "reconsider" the *Katz* test.[113]

Similar to both Justice Kennedy and Justice Thomas, Justice Alito contended the majority erred in preserving a person's Fourth Amendment right in "a third party's property."[114] The majority's holding "flouts the clear text of the Fourth Amendment."[115] He explained the "Fourth Amendment does not confer rights with respect to the persons, houses, papers, and effects of others."[116] Because Carpenter "ha[d] no meaningful control over the cell-site records, which are created, maintained, altered, used, and eventually destroyed by his cell service providers," he could not claim that they were his "papers" or "effects" for the purposes of Fourth Amendment protection.[117]

In contrast to the other dissenters, Justice Gorsuch took a more privacy-protective stance. However, he advocated for this privacy-protective approach

---

105. *Id.* at 2235 (Thomas, J., dissenting).

106. *Id.*

107. *Id.* at 2236.

108. *See id.*

109. *Id.*

110. As previously noted, the text of the Fourth Amendment states in part: "The right of the people to be secure in *their* persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ." U.S. CONST. amend. IV (emphasis added).

111. *Carpenter*, 138 S. Ct. at 2242 (Thomas, J., dissenting).

112. *Id.*

113. *Id.* at 2244, 2246.

114. *Id.* at 2257 (Alito, J., dissenting).

115. *Id.*

116. *Id.*

117. *Id.* at 2257, 2259.

with the Fourth Amendment. He explained from a "traditional" perspective, "Fourth Amendment protections for your papers and effects do not automatically disappear just because you share them with third parties."[118] Justice Gorsuch cited five arguments in support of this contention. For example, he cited bailment. Bailment involves "[e]ntrusting your stuff to others."[119] The "bailee normally owes a legal duty to keep the item safe" and if "[a] bailee . . . uses the item in a different way than he's supposed to, or against the bailor's instructions, [the bailee] is liable for conversion."[120] Justice Gorsuch explained "[j]ust because you entrust your data—in some cases, your modern-day papers and effects—to a third party may not mean you lose any Fourth Amendment interest in its contents."[121] Ultimately, he concluded that "[n]eglecting more traditional approaches may mean failing to vindicate the full protections of the Fourth Amendment."[122]

Contrary to the majority, the dissents advocate for a textual and property-centric understanding of the Fourth Amendment.

III. PRIVACY POLICIES

Post-*Carpenter*, the third-party doctrine's future is uncertain. Will the Court continue to dance around its application? Or, will the Court entertain its application in the context of a different question? This Note examines the ways in which the third-party doctrine can live on and how privacy policies can aid in sustaining it. While optimistic about its future, this Note acknowledges that the third-party doctrine will likely live on in an altered form. This section contributes to the argument that privacy policies perpetuate the third-party doctrine by providing a brief background on privacy policies. It will refer to Facebook's data policy and Uber's privacy policy for example purposes.

A privacy policy is "a written description posted on a company's Web site explaining how the company applies specific fair information practices to the collection, use, storage, and dissemination of personal information provided by visitors."[123] For example, when a new user signs up for Facebook, he or she

118. *Id.* at 2268 (Gorsuch, J., dissenting).

119. *Id.*

120. *Id.* at 2268–69.

121. *Id.* at 2269.

122. *Id.* at 2272.

123. Corey A. Ciocchetti, *E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors*, 44 AM. BUS. L.J. 55, 68 (2007); *see also* Mike Hintze, *Privacy Statements: Purposes, Requirements, and Best Practices*, *in* CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 413, 414 (Evan Selinger, Jules Polonetsky & Omer Tene eds., 2018) ("A privacy statement is primarily a legal document. It fulfils numerous, specific legal requirements imposed by a growing number of privacy laws and regulations worldwide. Conversely, it creates legal obligations, since inaccuracies in a privacy statement can lead to legal liability."); *Privacy Policy Law and Legal Definition*, USLEGAL, https://definitions.uslegal.com/p/privacy-policy (last visited Feb. 11, 2019) (defining a privacy policy as "a legal document that discloses some or all of the ways a party gathers, uses, discloses and manages a customer's data.").

agrees to the company's data policy.[124] Facebook's data policy answers questions such as: "[w]hat kinds of information do we collect," "[h]ow do we use this information," "[h]ow is this information shared," and "[h]ow do we respond to legal requests or prevent harm?"[125] Uber follows suit. A new rider must agree to its privacy policy to use its service. In its privacy policy, Uber explains items such as what information it collects, how it uses information, how it shares information, how it utilizes cookies and related technologies, and how it retains information.[126]

A defining feature of privacy law in the United States is its sectoral approach.[127] The United States does not have "privacy laws . . . [that] protect all personal data in an omnibus fashion," but "different laws regulating different industries and economic sectors."[128] This regime "leaves large areas unregulated, especially at the federal level."[129] For example, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulates health care sector privacy policies and the Gramm-Leach-Bliley Act of 1999 (GLBA) regulates the financial sector privacy policies.[130] However, "there is no federal law that directly protects the privacy of data collected and used by merchants such as Macy's and Amazon.com. Nor is there a federal law focused on many of the forms of data collection in use by companies such as Facebook and Google."[131] Thus, "unregulated sectors are left under the watch of the [Federal Trade Commission]."[132]

The Federal Trade Commission (FTC) is a federal agency with a mission to "[p]rotect[] consumers and competition by preventing anticompetitive, deceptive, and unfair business practices through law enforcement, advocacy, and education without unduly burdening legitimate business activity."[133] It "has the authority . . . to enforce privacy policy promises under its general unfair and

124. *See Data Policy*, *supra* note 1.

125. *Id.*

126. *See Privacy Policy*, *supra* note 1.

127. *See* Ciocchetti, *supra* note 123, at 73 ("On a national level, Congress has chosen to regulate electronic privacy policies through sectoral legislation.").

128. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 587, 590 (2014) ("Today, scholars and practitioners almost take for granted that a privacy policy is a separate document, not a contract or even a set of privately enforceable promises, and that the FTC is the primary enforcer.").

129. *Id.* at 587.

130. *See* Ciocchetti, *supra* note 123, at 73–74.

131. Solove & Hartzog, *supra* note 128, at 587.

132. Ciocchetti, *supra* note 123, at 73; *see also* Solove & Hartzog, *supra* note 128, at 588 ("Because so many companies fall outside of specific sectoral privacy laws, the FTC is in many cases the primary source of regulation.").

133. *About the FTC*, FED. TRADE COMMISSION, https://www.ftc.gov/about-ftc (last visited Mar. 14, 2019).

deceptive practice powers."[134] In exercising these powers, the FTC purports a "notice and choice" approach.[135] The notice-and-choice approach is quite literally comprised of (1) notice and (2) choice. This approach "requires an information collector to disclose to an individual what personal information it proposes to collect from her and how it proposes to use that information ('notice')" and "afford[s] the individual an opportunity to prevent the collection of her [personally identifiable information] by denying consent or by declining to enter into the transaction ('choice')."[136] Notice and choice seemingly stand in the shoes of a formal regulatory system; this approach "is designed and promoted as a replacement for regulation."[137]

In addition to encouraging the notice-and-choice approach, the FTC facilitates the protection of consumers from "deceptive" and "unfair business practices" through enforcement actions.[138] The FTC's authority to bring such action stems from the Federal Trade Commission Act which "established the FTC and sought to protect American consumers from wrongful business practices."[139] Specifically, this Act "prohibits unfair and deceptive acts or practices in interstate commerce."[140] Thus, the FTC's power is restricted to two realms: unfair and deceptive practices.[141] In practice, the FTC's enforcement

134. Ciocchetti, *supra* note 123, at 73; *see also* Solove & Hartzog, *supra* note 128, at 585 ("Since the late 1990s, the Federal Trade Commission . . . has been enforcing companies' privacy policies through its authority to police unfair and deceptive trade practices.").

135. Reidenberg et al., *Disagreeable Privacy Policies*, *supra* note 6, at 42 ("In the United States, notice and choice has become the principal means to address privacy online."). For criticisms of this privacy approach, see Joel R. Reidenberg et al., *Privacy Harms and the Effectiveness of the Notice and Choice Framework*, 11 I/S 485, 490–96 (2015) [hereinafter Reidenberg et al., *Privacy Harms*]; John A. Rothchild, *Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online (or Anywhere Else)*, 66 CLEV. ST. L. REV. 559 (2018); Robert H. Sloan & Richard Warner, *Beyond Notice and Choice: Privacy, Norms, and Consent*, 14 J. HIGH TECH. L. 370 (2014).

136. Rothchild, *supra* note 135, at 561–62; *see also* Reidenberg et al., *Disagreeable Privacy Policies*, *supra* note 6, at 41 ("The idea is that companies post their privacy policies, users read and understand these policies, and then users follow a rational decision-making process to engage only with companies they believe offer an acceptable level of privacy.").

137. Reidenberg et al., *Disagreeable Privacy Policies*, *supra* note 6, at 41–42.

138. *See* Reidenberg et al., *Privacy Harms*, *supra* note 135, at 496 ("[W]hen the FTC perceives commercial practices that cause significant harm to consumers, the agency will bring enforcement actions.").

139. *Id.* at 508.

140. Ciocchetti, *supra* note 123, at 93.

141. *See* Reidenberg et al., *Privacy Harms*, *supra* note 135, at 509 ("The enabling statute's limitation to unfair and deceptive practices severely circumscribes the agency's authority over online privacy issues."); *see also* Ciocchetti, *supra* note 123, at 94 ("Although the FTC does not require companies to post privacy policies, it has the authority to bring an enforcement action as either an unfair or a deceptive practice, or both, if promises are made and subsequently broken.").

actions primarily pertain to deceptive practices.[142] In these deceptive practices actions, the FTC evaluates "whether or not a person or company broke a promise or engaged in a misleading act."[143] Essentially, "[u]nder this deception theory, a company would be permitted, without repercussion, either to tell consumers whether and how their personal information will be exploited, provided it upholds its word; or to promise them nothing about their online privacy at all."[144] The FTC typically steps in when a company breaks a promise it has made to a user in its privacy policy.[145] It tends to give a slap on the wrist in the form of a fine.[146]

The notice-and-choice approach and the FTC's enforcement role highlight a unique tension. The notice-and-choice approach is meant to empower the user: it provides a user to the tools to make a thoughtful decision.[147] However, enforcement actions incentivize companies to pen broad privacy policies with minimal user protections or to opt out of such practices altogether.[148] Though well-intentioned, the mechanisms meant to protect users seemingly impede their privacy rights.

IV. HOW PRIVACY POLICIES PERPETUATE THE THIRD-PARTY DOCTRINE

Ultimately, privacy policies, such as that of Facebook and Uber, perpetuate the third-party doctrine. The Fourth Amendment only offers protection to a person's own property. When the property of another is at issue, the third-party doctrine applies. Privacy policies operate as a sort of switching or conversion mechanism. In the context of a property-centric understanding of the Fourth Amendment and the United States' notice-and-choice scheme, privacy policies transform an individual's personal information into business

142. *See* Reidenberg et al., *Privacy Harms*, *supra* note 135, at 510 ("Not surprisingly, the FTC invokes unfairness less frequently than it invokes deception. This is because unfair practices are often harder to demonstrate and prove as compared to deceptive practices.").

143. *Id.* at 509.

144. *Id.*

> Under self-regulation, businesses essentially determined for themselves the basic rules they will adhere to regarding data collection, use, and disclosure. They stated these rules in their privacy policies. FTC enforcement added some teeth to the promises in privacy policies, most of which lacked any penalty or consequence if a company failed to live up to its promises.

Solove & Hartzog, *supra* note 128, at 604.

145. *See* Reidenberg et al., *Privacy Harms*, *supra* note 135, at 509.

146. *See* Solove & Hartzog, *supra* note 128, at 605 (explaining "[a]bsent such grounds for issuing a civil penalty, the FTC is limited to fining companies under a contempt action for violating a settlement order" and "[w]hen the FTC does include fines, they are often quite small in relation to the gravity of the violations and the overall net profit of the violators. . . . [B]ecause any fines issued by the FTC must reflect the amount of consumer loss.").

147. *See* Reidenberg et al., *Privacy Harms*, *supra* note 135, at 496 ("The intent of a notice and choice regime is to enable users to make meaningful, informed decisions regarding their privacy.").

148. *See id.* at 509.

records or the property of a company. Three privacy policy provisions contribute to this transformation: (1) the information-collection notice, (2) the information-use notice, and (3) the legal provision. When users are notified of what information is collected, how the information is used, and how the information can be shared and then choose to agree to these practices, personal information is conceptually converted into business records or company property. Thus, a Fourth Amendment claim is inapplicable. The third-party doctrine applies.

Privacy policies do not operate in isolation. The argument that privacy policies perpetuate the third-party doctrine relies on a property-centric understanding of the Fourth Amendment. It is also depends upon the United States' notice-and-choice approach to privacy. Thus, the following material first examines the legal landscape that creates a favorable environment for the continued application of the third-party doctrine. Next, it analyzes the three transformative privacy policy provisions and contemplates the third-party doctrine in the absence of such policies. Finally, it considers the potential reformulation of the third-party doctrine for future application by the courts. Combining the legal context and privacy policies, this portion of the Note will demonstrate how privacy policies perpetuate the third-party doctrine. The following sections will refer to Facebook's data policy and Uber's privacy policy, where applicable, for example purposes.

A. The Legal Landscape

1. The Fourth Amendment: A Property-Centric Approach

The property-centric understanding of the Fourth Amendment emerges from *Smith*, *Miller*, and the *Carpenter* dissents. This view represents a more traditional, textual interpretation of the Fourth Amendment. Simply stated by Justice Thomas in his *Carpenter* dissent, this approach contemplates "*whose* property was searched."[149] As pointed out by Justice Thomas, the Fourth Amendment offers protection to people in "*their* persons, houses, papers, and effects."[150] It does not provide a person with rights in the property of another.[151] Thus, if an individual's own property is searched, he or she can assert his or her Fourth Amendment rights. However, if another's property is searched, an individual cannot assert his or her Fourth Amendment rights in the property of a third party. Both the Fourth Amendment and the third-party doctrine mandate this result.

Miller says an individual has no protectable Fourth Amendment interest in the "business records" of a third party.[152] The "documents subpoenaed [in that case were] not respondent's 'private papers'" but "the business records of

149. Carpenter v. United States, 138 S. Ct. 2206, 2235 (2018) (Thomas, J., dissenting).

150. U.S. CONST. amend. IV (emphasis added); *see also Carpenter*, 138 S. Ct. at 2241–42 (Thomas, J., dissenting).

151. *Carpenter*, 138 S. Ct. at 2242 (Thomas, J. dissenting).

152. United States v. Miller, 425 U.S. 435, 440 (1976).

the banks."[153] Similarly, in *Smith*, when information was voluntarily shared with a third party, there was no valid Fourth Amendment interest because it could be expected that the company would retain the information for business uses.[154] Turning to *Carpenter*, the dissenting opinions echo a similar sentiment. Justice Kennedy explains that Fourth Amendment protections are restricted to an individual's own property.[155] He also focuses on the "business records" argument articulated in *Miller* and explains that an individual cannot assert a property interest in such records of a third party.[156] Both Justice Thomas and Justice Alito also argue that the Fourth Amendment only protects an individual's own property.[157] Like the other Justices, Justice Gorsuch also advocates for a traditional understanding of the Fourth Amendment.[158]

Justice Gorsuch departs from the rest of the dissenters on the question of when a certain type of property becomes the property of a third party. Justice Kennedy, Justice Alito, and Justice Thomas seemingly say if a person willingly shares information with a third party for business purposes, the information can qualify as a business record. An individual forfeits Fourth Amendment rights in such business records. On the other hand, Justice Gorsuch explains, "just because you *have* to entrust a third party with your data doesn't necessarily mean you should lose all Fourth Amendment protections in it."[159]

Though the dissents ultimately diverge from one another, these three cases—*Miller*, *Smith*, and *Carpenter*—each advocate for a traditional and textual property-centric understanding of the Fourth Amendment. As compared to *Katz's* liberal Fourth Amendment test, the property-centric approach to the Fourth Amendment restricts the reach of this constitutional provision to a person's own property—not property in which an individual subjectively believes he or she has a societally-approved interest.[160] Thus, this property-centric approach enables the continued application of the third-party doctrine by reinforcing the concept that a person does not have a constitutionally protected interest in the property of another.

2. Notice and Choice

Supported by the FTC, notice and choice is the prevailing privacy practice in the United States.[161] The notion of notice involves the "presentation of terms" and the concept of choice involves "an action signifying acceptance of the terms."[162] This approach holds users must be informed about how their

153. *Id.*
154. Smith v. Maryland, 442 U.S. 735, 743–44 (1979).
155. *Carpenter*, 138 S. Ct. at 2227 (Kennedy, J., dissenting).
156. *Id.* at 2229–30.
157. *Id.* at 2242 (Thomas, J., dissenting); *id.* at 2257 (Alito, J., dissenting).
158. *Id.* at 2267–68 (Gorsuch, J., dissenting).
159. *Id.* at 2270.
160. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
161. *See* Sloan & Warner, *supra* note 135, at 374–75.
162. *Id.* at 373–74.

information is obtained, utilized, and disseminated such that they can decide whether or not to continue using a website.[163] For example, Facebook notifies a potential user: "This policy describes the information we process to support Facebook, Instagram, Messenger and other products and features offered by Facebook . . . ."[164] Similarly, Uber educates a prospective rider: "This policy describes how Uber and its affiliates collect and use personal information to provide our services."[165] Essentially, the notice-and-choice approach places the ball in the user's court. Once a company provides certain notices regarding its practices, it is up to the user to decide whether to consent or forego the use of the service. This practice enables the continued application of the third-party doctrine because it basically garners a user's consent to the use of his or her personal information for business purposes or as part of business records. With notice and choice, users consent to the conversion of their personal information into the property of another. Thus, users' information is not necessarily within the reach of Fourth Amendment protections but in the realm of the third-party doctrine.

B. How Privacy Policies Perpetuate Third-Party Doctrine: Three Key Provisions

By way of reminder, a privacy policy "describe[s] the various ways in which websites collect[], use[], and share[] a visitor's personal information, as well as the various ways that information [is] protected."[166] In light of the above-mentioned legal landscape, privacy policies themselves perpetuate the third-party doctrine. They accomplish this feat primarily through three provisions.[167] The following section will separately address each provision.

First, the information-collection provision. This portion of a privacy policy notifies a user of the kind of information a company collects. Facebook collects a wealth of information. According to its data policy, Facebook stores information regarding user-provided information, user-provided content, networks, connections, usage, transactions, devices, and "[i]nformation from partners."[168] For example, from the "[i]nformation and content [users] provide," Facebook collects "the content, communications and other information you provide," which "can include information in or about the content you provide (like metadata), such as the location of a photo or the date a file was created."[169] Facebook also gleans information from "[a]dvertisers, app developers, and publishers" who "provide information about your activities off Facebook—including information about your device, websites you visit,

163. *See id.*

164. *Data Policy*, *supra* note 1.

165. *Privacy Policy*, *supra* note 1.

166. Solove & Hartzog, *supra* note 128, at 592.

167. Privacy policies typically contain numerous provisions. For a listing and explanation of the types of provisions that such policies can contain, see generally Hintze, *supra* note 123.

168. *Data Policy*, *supra* note 1.

169. *Id.*

purchases you make, the ads you see, and how you use their services—whether or not you . . . are logged into Facebook."[170] Similarly, Uber collects a bevy of biographical user information. It collects information from a rider's profile and information related to location, transactions, usage, devices, and communications.[171] For example, Uber can "collect your precise or approximate location information as determined through data such as GPS, IP address and WiFi."[172] With this provision, a company is notifying a user what information it is collecting for business purposes.

Second, the information-use provision. This provision describes how a company uses the information it has collected. "Common uses include: [o]perating and providing the product(s) and/or service(s), [i]mproving the product(s) and service(s), [g]eneral business operations, [s]ecurity . . . , [p]ersonalization . . . , [d]irect marketing, and [a]dvertising."[173] Essentially, companies like Facebook and Uber use the information for business purposes. These companies leverage the information they have obtained to improve their services and offerings.

Facebook uses the information it has collected to "[p]rovide measurement, analytics, and other business services."[174] Specifically, it uses user information "to help advertisers and other partners measure the effectiveness and distribution of their ads and services, and understand the types of people who use their services and how people interact with their websites, apps, and services."[175] In the same vein, Uber uses rider information to "provide, personalize, maintain and improve our products and services," "for testing, research, analysis and product development. . . . [T]o improve and enhance the safety and security of our services, develop new features and products, and facilitate insurance and finance solutions in connection with our services," and to "help maintain the safety, security and integrity of our services and users."[176] By inserting such provisions into their privacy policies, a company like Facebook or Uber is notifying a user that his or her information is being used for business purposes (i.e., creating business records).

Third, the legal provision. This term details how a company can share the information it has collected with parties listed in the privacy policy. However,

---

170. *Id.* It was relatively recently revealed that certain applications were sending users' personal information to Facebook. For greater insights into this issue, see Sam Schechner & Mark Secada, *You Give Apps Sensitive Personal Information. Then They Tell Facebook.*, WALL ST. J. (Feb. 22, 2019, 11:07 AM), https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636?mod=article_inline; Sam Schechner, *Popular Apps Cease Sharing Data with Facebook*, WALL ST. J. (Feb. 24, 2019, 5:46 PM), https://www.wsj.com/articles/popular-apps-cease-sharing-data-with-facebook-11551044791?mod=searchresults&page=6&pos=8.

171. *Privacy Policy*, *supra* note 1.

172. *Id.*

173. Hintze, *supra* note 123, at 416.

174. *Data Policy*, *supra* note 1.

175. *Id.*

176. *Privacy Policy*, *supra* note 1.

this Note is specifically concerned with how information is shared with the authorities and for other legal purposes. Both Facebook and Uber permit the sharing of information with legal authorities in enumerated circumstances. The legal provisions from Facebook's data policy and Uber's privacy policy are set forth in full below.

1. Facebook

> We access, preserve and share your information with regulators, law enforcement or others:
>
> In response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so. This may include responding to legal requests from jurisdictions outside of the United States when we have a good-faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognized standards.
>
> When we have a good-faith belief it is necessary to: detect, prevent and address fraud, unauthorized use of the Products, violations of our terms or policies, or other harmful or illegal activity; to protect ourselves (including our rights, property or Products), you or others, including as part of investigations or regulatory inquiries; or to prevent death or imminent bodily harm. For example, if relevant, we provide information to and receive information from third-party partners about the reliability of your account to prevent fraud, abuse and other harmful activity on and off our Products.
>
> Information we receive about you (including financial transaction data related to purchases made with Facebook) can be accessed and preserved for an extended period when it is the subject of a legal request or obligation, governmental investigation, or investigations of possible violations of our terms or policies, or otherwise to prevent harm. We also retain information from accounts disabled for terms violations for at least a year to prevent repeat abuse or other term violations.[177]

2. Uber

> Uber may share your information if we believe it is required by applicable law, regulation, operating agreement, legal process or governmental request, or where the disclosure is otherwise appropriate due to safety or similar concerns.
>
> This includes sharing your information with law enforcement officials, government authorities, airports (if required by the airport authorities as a condition of operating on airport property), or other

177. *Data Policy*, *supra* note 1.

> third parties as necessary to enforce our Terms of Service, user agreements, or other policies, to protect Uber's rights or property or the rights, safety or property of others, or in the event of a claim or dispute relating to your use of our services. If you use another person's credit card, we may be required by law to share information with that credit card holder, including trip information.
>
> This also includes sharing your information with others in connection with, or during negotiations of, any merger, sale of company assets, consolidation or restructuring, financing, or acquisition of all or a portion of our business by or into another company.[178]

The broad language of these sweeping provisions allows Facebook and Uber to share user information with the authorities and for other legal purposes when a low bar is met: subjective belief. With such legal provisions, a company is explaining to a user how his or her information can be shared with others. Thus, by agreeing to a privacy policy, a user permits the sharing of his or her personal information.

The aforementioned privacy policy provisions function as a triple-threat, transforming personal information into business records. The information-collection provision notifies a user what information the company is collecting. The information-use provision explains how the company is using the information. It tells the user that his or her information will be used for business purposes. When contained in a "user profile" for a company like Uber, personal information is easily construed as a component of a business record.[179] Finally, the legal provision permits a company to share personal information in a wide variety of circumstances. In many cases, it only requires that the company have a subjective "good-faith belief" to share information with the authorities or for other legal purposes.[180]

A privacy policy provides a user with ample notice. Thus, when a user chooses to agree to a privacy policy, he or she says the organization may collect his or her information, use it for business purposes, and share it with others (including the government, whether or not it has a search warrant). After acknowledging such terms, it is unpersuasive for a user to attempt to assert a Fourth Amendment claim with respect to such information. A user has already agreed that the information may be collected, used, and shared for business purposes. His or her information has been transformed into a business record. It is the property of a third party and in the province of the third-party doctrine. In this way, privacy policies perpetuate the third-party doctrine.

178. *Privacy Policy*, *supra* note 1.

179. *Id.*

180. *See Data Policy*, *supra* note 1.

C. Legal Claims in the Absence of Privacy Policies

The above contends that privacy policies perpetuate the third-party doctrine. But, what if privacy policies did not exist? What would a third-party doctrine claim look like in the absence of privacy policies? In such a scenario, how would a user's personal information be treated when shared with a company like Facebook or Uber? A user's information would likely be treated in one of two ways.

First, a court could engage in a fact-specific inquiry. Privacy policies govern a user's expectation of how a company will use his or her information. Without this governing document, a court must dive into the facts and consider questions such as whether the user intended to share his or her personal information, what kind of information was shared, whether the company used the information in a foreseeable way, and to whom the information belongs. In the absence of privacy policies, fact-specific inquiries by the courts could lead to inconsistencies such that in some cases user information is protected and in other cases it is unprotected.

Second, a court could take the voluntary disclosure route. It could simply point to the user's voluntary disclosure of information to a third party to support the contention that the user does not have a privacy interest in the information shared. Like a typical third-party doctrine claim, because the user turned over his or her information to another, a user forfeits his or her privacy rights in the information. As opposed to the first option, the question of voluntary disclosure is easier to apply to an array of facts. However, it could represent an oversimplification of the many important questions a court should answer regarding a user's personal information sans privacy policies. Further, post-*Carpenter*, the degree of persuasiveness of a user's voluntary disclosure in the context of a legal inquiry is an open question.

Essentially, in the absence of privacy policies, it is unclear how a user's personal information and privacy rights in that information will be handled in the context of the third-party doctrine. However, it is likely that the lack of privacy policies could create inconsistencies in the treatment of a user's personal information. By setting expectations for both users and companies as to how personal information will be used, privacy policies can aid in avoiding fact-specific inquiries by courts (also creating judicial efficiency) and prevent the oversimplification of key legal questions.

D. A Path Forward for the Third-Party Doctrine

While tools like privacy policies perpetuate the third-party doctrine, discontent with the doctrine in its current form is evident. It holds: an individual "has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[181] The apparent issue with the third-party doctrine seems to stem from the Fourth Amendment.

---

181. Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018) (quoting Smith v. Maryland, 442 U.S. 735, 743–44 (1979)).

The *Carpenter* majority explained: "Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection."[182] The *Carpenter* dissents took issue with how far the Fourth Amendment has strayed from its roots in the text of the Constitution.[183] Justice Kennedy wrote that the majority's interpretation "unhinges Fourth Amendment doctrine from the property-based concepts that have long grounded the analytic framework that pertains in these cases."[184] Justice Thomas identified that a "fundamental problem" is the "'reasonable expectation of privacy' test, which was first articulated by Justice Harlan in *Katz v. United States*."[185] He continued, "[t]he *Katz* test has no basis in the text or history of the Fourth Amendment" and "[u]ntil we confront the problems with this test, *Katz* will continue to distort Fourth Amendment jurisprudence."[186] As described in Part I, the "legitimate expectation of privacy" concept is common to both the *Katz* test and the third-party doctrine.[187] Extrapolating the dissents' dissatisfaction with this test from the Fourth Amendment context to that of the third-party doctrine, to continue on, the third-party doctrine should shed its "legitimate expectation of privacy"[188] test. In its place, the courts should incorporate the property-centric view of the Fourth Amendment.

A revised third-party doctrine could contain two prongs. Instead of asking whether an individual has a "legitimate expectation of privacy,"[189] it could contemplate (1) "*whose* property was searched"[190] and (2) whether the property or information obtained was voluntarily shared.[191] This reformulation of the third-party doctrine ties it to the text of the Fourth Amendment. It also simplifies the legal inquiry. If an individual's own property is in question, the Fourth Amendment applies. If a third party's property is at issue, the third-party doctrine will apply.

The benefit of this approach is the discernment phase in which the true property owner is determined. In these technological times, the courts will have to tease out this ownership question. Privacy policies are integral to this inquiry as they dictate information ownership in the technology realm. As noted above, privacy policies govern the collection, use, and legal treatment of information. They are currently one-sided: the company is owner.

---

182. *Id.* at 2217.

183. *See generally id.* at 2223–72.

184. *Id.* at 2224 (Kennedy, J., dissenting).

185. *Id.* at 2236 (Thomas, J., dissenting) (citation omitted) (citing Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring)).

186. *Id.*

187. *See* United States v. Miller, 425 U.S. 435, 442 (1976).

188. *See id.*

189. *See id.*

190. *Carpenter*, 138 S. Ct. at 2235 (Thomas, J., dissenting).

191. *See id.* at 2216.

As the amount of user information a company collects continues to increase, complete company ownership of information is unrealistic. There is a need for privacy policy reform. There are a number of ways to accomplish this reform. The government could regulate privacy policies and specifically define user rights related to information. The FTC could pivot from enforcer to proactive and preventative regulator. In the alternative, companies could self-regulate privacy policies. Companies could allow users to select which personal information could be used for business purposes. Companies could also accomplish this by altering the legal provisions. Instead of requiring a "good-faith belief"[192] to share information with legal parties, companies could establish a higher bar and part with a user's personal information only in response to a warrant.

Whether implemented via government regulation or by companies themselves, clear and equitable definition of information ownership could contribute to the effective implementation of the reformulated third-party doctrine going forward. Such definition increases users' privacy rights and creates judicial efficiency by simplifying the legal question "*whose* property was searched."[193] Ultimately, the path forward for the third-party doctrine can be found in reformulation of both the doctrine itself and privacy policies.

CONCLUSION

Another *Carpenter*-esque question is likely to confront the courts in the near future. The *Carpenter* Court strategically sidestepped the third-party doctrine by applying *Knotts* and *Jones*. However, in the appropriate context, a court should not shy away from but seize the opportunity to engage with the third-party doctrine. Courts should leverage the notion that privacy policies perpetuate the third-party doctrine to their advantage. A reformulated third-party doctrine, along with revised privacy policies, can and should be used to more clearly define and protect privacy rights.

192. *Data Policy*, *supra* note 1.

193. *Carpenter*, 138 S. Ct. at 2235 (Thomas, J., dissenting).