Article

Contracting for Fourth Amendment Privacy Online

Wayne A. Logan† and Jake Linford††

† Gary & Sallyn Pajcic Professor of Law, Florida State University College of Law.

†† Loula Fuller & Dan Myers Professor of Law, Florida State University College of Law. Thanks very much to James Grimmelmann, Jay Kesten, Richard Re, Ric Simmons, Christopher Slobogin, Matthew Tokson, and Ari Ezra Waldman for their helpful comments.

INTRODUCTION

In January 2019, Facebook and Instagram users responded in droves to a new viral invitation to share their information online. To participate in the #10YearChallenge, users posted a picture from ten years ago to compare with a current photograph.[1] Although a seemingly innocuous undertaking, privacy experts expressed concern that Facebook was yet again manipulating its users to secure financial gain, this time to develop and expand facial recognition algorithms and optimize age progression technology.[2] Improving facial recognition tools would allow the company to both better mine facial data to increase the efficacy of predictive technologies, and perhaps sell the technology to others, including law enforcement.[3]

Today, the internet ecosystem figures centrally in everyday existence. Even the Supreme Court, an institution not known for its tech-savviness,[4] has recognized the core role of social media platforms like Facebook and online access tools like smartphones in contemporary social and civic life.[5] It should therefore come as no surprise that law enforcement, engaged in the "competitive

1. *See, e.g.*, Arwa Mahdawi, *Think the #10YearChallenge is Fun? It's a Surveillance Nightmare*, THE GUARDIAN (Jan. 18, 2019, 1:14 pm), https://gu.com/p/afmqh/stw [https://perma.cc/HG4L-RL7T]; Kate O'Neill, *Facebook's '10 Year Challenge' is Just a Harmless Meme—Right?*, WIRED (Jan. 15, 2019, 6:39 pm), https://www.wired.com/story/facebook-10-year-meme-challenge/ [https://perma.cc/SU83-NVMS].

2. *See* Mahdawi, *supra* note 1; O'Neill, *supra* note 1.

3. *See* Mahdawi, *supra* note 1; O'Neill, *supra* note 1. Similarly, Amazon was recently criticized by its own employees for a deal to sell its facial recognition technology to law enforcement agencies. *See* Thomas Brewster, *Amazon Employees Ask Bezos to Stop Selling Facial Recognition to Cops*, FORBES, (June 22, 2018, 6:10 AM), https://www.forbes.com/sites/thomasbrewster/2018/06/22/amazon-staff-demand-company-stop-selling-facial-recognition-to-police/ [https://perma.cc/TJ96-2QUP].

4. *See* Mark Grabowski, *Are Technical Difficulties at the Supreme Court Causing a "Disregard of Duty"?*, 3 CASE W. RES. J.L. TECH. & INTERNET 93, 93 (2012) ("Recent U.S. Supreme Court cases involving technology-related issues indicate that several Justices are embarrassingly ignorant about computing and communication methods that many Americans take for granted.").

5. *See, e.g.*, Packingham v. North Carolina, 137 S. Ct. 1730, 1737 (2017) (likening social media platforms such as Facebook to the "modern public square"); Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (5-4 decision) (quoting Riley v. California, 134 S. Ct. 2473, 2484 (2014)) ("[C]ell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society.").

enterprise of ferreting out crime,"[6] will scour the Internet for potentially incriminating information. Indeed, police today often insinuate themselves into social media platforms by pretending to be a "friend"; pressure an actual friend of a user to disclose information; and access content stored by an individual on the Cloud.[7]

On their face, such police behaviors would appear permissible as a matter of Fourth Amendment doctrine. Invoking the third party doctrine, courts have long viewed the voluntary sharing of information with others as negating any privacy expectation in that information.[8] The doctrine has been the subject of widespread condemnation by commentators,[9] and only narrowly escaped its demise last Term in *Carpenter v. United States*.[10] In *Carpenter*, police, acting without a search warrant, accessed from a cell phone service provider locational geo-information that the defendant's cell phone generated, and used the information to place the defendant near the site of several robberies. The Supreme Court held that the fact that the information was collected and maintained by cell phone service providers—third parties—did "not make it any less deserving of Fourth Amendment protection."[11] The five-member majority, however, refused

6. Johnson v. United States, 333 U.S. 10, 14 (1947).

7. See, e.g., Rachel Levinson-Waldman, *Government Access to and Manipulation of Social Media: Legal and Policy Challenges*, 61 HOW. L.J. 523, 524–31 (2018) (providing examples).

8. *See* United States v. Miller, 425 U.S. 435, 443 (1976) (noting that there is no privacy expectation "even if the information is revealed on the assumption that it will be used only for a limited purpose"); Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties. . . ."); *see also* Katz v. United States, 389 U.S. 347, 351 (1967) ("[T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.").

9. *See, e.g.*, Jane Bambauer, *Other People's Papers*, 94 TEX. L. REV. 205, 214 n.51 (2015) (cataloging many critiques of the doctrine); Andrew J. DeFilippis, *Securing Informationships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence*, 115 YALE L.J. 1086, 1097–1108 (2006) (challenging the third-party doctrine); Stephen E. Henderson, *After* United States v. Jones*, After the Fourth Amendment Third Party Doctrine*, 14 N.C. J.L. & TECH. 431, 431–34 (2013) (same); Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 113 (2008) (same). *But see* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 562 (2009) [hereinafter Kerr, *Third-Party Doctrine*] (defending the third-party doctrine).

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

11. *Id.* at 2217, 2223.

to formally renounce the third party doctrine, terming its decision a "narrow one,"[12] based on "the unique nature of cell phone location records."[13]

While the Court and commentators continue to debate the third party doctrine, an important shift has escaped notice: state and lower federal courts are hollowing out the third party doctrine from below as they reject, or at least question, the doctrine's impact in the context of the Internet.[14] Scrutinizing terms of service agreements and "privacy settings" selected by individual users, courts are reconceiving what it means to "voluntarily turn[] over"[15] information to others in the Internet Age.[16] In this Article, we describe this emerging body of case law and elaborate upon and defend courts' use of contract law as an analytic tool in addressing whether users possess a Fourth Amendment privacy right in their shared information.

That principles of contract law should apply in Fourth Amendment doctrine is not as novel as it might first appear.[17] Indeed, Professor William Stuntz, writing well before the full emergence of the Internet and social media platforms, advocated a contract-like analytic model asking, "[w]hat search rule would the government and innocent targets adopt if they were to negotiate the rule in advance?"[18] Half a century earlier, Justice Pierce

12. *See id.* at 2220 ("We do not express a view on matters not before us . . . . We do not disturb the application of *Smith* and *Miller* [the Court's landmark third party doctrine precedent] or call into question conventional surveillance techniques and tools, such as security cameras.").

13. *Id.* at 2217; *see also id.* at 2220 ("Given the unique nature of cell phone location information, the fact that the Government obtained the information from a third party does not overcome Carpenter's claim to Fourth Amendment protection."). *But see id.* at 2267 (Gorsuch, J., dissenting) ("[A]pparently *Smith* and *Miller* aren't quite left for dead; they just no longer have the clear reach they once did.").

14. On the phenomenon more generally, see Richard M. Re, *Narrowing Supreme Court Precedent from Below*, 104 GEO. L.J. 921 (2016).

15. Smith v. Maryland, 442 U.S. 735, 744 (1979).

16. *Carpenter*, 138 S. Ct. at 2216.

17. *See, e.g.*, William J. Stuntz, *Implicit Bargains, Government Power, and the Fourth Amendment*, 44 STAN. L. REV. 553 (1992).

18. *Id.* at 555; *see also* Bernard W. Bell, *Secrets and Lies: News Media and Law Enforcement Use of Deception as an Investigative Tool*, 60 U. PITT. L. REV. 745, 774–75 (1999) (arguing that state and local laws and customs, including property interests defined by contract, should set baseline privacy expectations in a given locality); Steven A. Bibas, *A Contractual Approach to Data Privacy*, 17 HARV. J.L. & PUB. POL'Y 591, 605–11 (1994) (proposing a contractual approach for data privacy).

Butler, dissenting in *Olmstead v. United States*,[19] opined that contracts between telephone companies and their consumers should govern privacy expectations.[20] Indeed, the Supreme Court itself has held that "property concepts" play a role in determining whether a reasonable expectation of privacy exists,[21] and that contract rights are a form of property.[22] Modern legal commentators, for their part, have argued in general that the third party doctrine is ill-suited to the social media context,[23] but made only fleeting reference to the potential utility of contract doctrine in assessing Fourth Amendment claims.[24]

The Article proceeds as follows: Part I lays the foundation by examining the third party doctrine, which arose and evolved in an era when face-to-face human interaction was the business and interpersonal norm. In its strong form, the doctrine dictates that any voluntary exposure of information by an individual to others negates any privacy expectation in the information.[25]

Part II surveys the increasing number of courts that have applied the third party doctrine to the online environment. To be sure, many take a traditional approach, regarding any voluntary exposure, or potential exposure, as a basis to reject a privacy expectation. Other courts, however, interpret the third party doctrine more narrowly, and attach importance to whether a user

19. 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1976), *and* Berger v. New York, 388 U.S. 41 (1967).

20. *See id.* at 487 ("The contracts between telephone companies and users contemplate the private use of the facilities employed in the service . . . . During their transmission the exclusive use of the wire belongs to the persons served by it. Wiretapping involves interference with the wire while being used.").

21. *See* Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978) (noting that "property concepts" are instructive in "determining the presence or absence of the privacy interests protected by th[e Fourth] Amendment").

22. U.S. Tr. Co. of N.Y. v. New Jersey, 431 U.S. 1, 19 n.16 (1977) (recognizing that "[c]ontract rights are a form of property").

23. *See, e.g.*, Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211, 258–59 (2006); Woodrow Hartzog, *The Fight to Frame Privacy*, 111 MICH. L. REV. 1021, 1028–29 (2013) (book review); Brian Mund, *Social Media Searches and the Reasonable Expectation of Privacy*, 19 YALE J.L. & TECH. 238, 238 (2017).

24. *See* Randy Barnett, *Why the NSA Data Seizures Are Unconstitutional*, 38 HARV. J.L. & PUB. POL'Y 3, 13 (2015) ("[B]y availing themselves of the law of property and contract, people create their own zones of privacy. In short, *first comes property and contract, then comes privacy*.") (emphasis in original).

25. *See* Henderson, *supra* note 9, at 432.

has expressed a privacy preference. These cases signal a willingness to reconsider the baseline presumptions of the third party doctrine about what it means to voluntarily share information in the Internet Age. Some courts take a similarly critical approach to terms of service and user agreements, narrowly interpreting the often broad language they contain. In both contexts, a privacy expectation can exist even in the face of a risk that: (1) another individual, trusted with the information, will provide information to police or (2) the user "misplaces confidence" in another who actually turns out to be an undercover officer.[26] Individuals, in short, do not necessarily "assume the risk" that law enforcement will obtain and use their information, as the third party doctrine would require.[27]

Part III moves from the descriptive to the prescriptive, pointing a way forward in what courts acknowledge to be shifting terrain,[28] amid continued dissatisfaction with the *Katz* reasonable expectation of privacy test,[29] which has long governed Fourth Amendment privacy analysis.[30] After noting that contract law principles have in fact often figured into Fourth Amendment jurisprudence, we argue that those principles can and should play a more central role in assessing privacy rights in the online environment. We then consider the questions raised by the case law in Part II in light of contract principles, especially regarding interpretation of boilerplate text and user

26. *See infra* Part II.A–B.

27. As the Sixth Circuit Court of Appeals stated in a recent case, "the threat or possibility of access is not decisive when it comes to the reasonableness of an expectation of privacy." United States v. Warshak (*Warshak III*), 631 F.3d 266, 287 (6th Cir. 2010); *see also* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) ("A person does not surrender all Fourth Amendment protection by venturing into the public sphere.").

28. *See, e.g.*, *Carpenter*, 138 S. Ct. at 2213–14 (acknowledging that "no single rubric definitively resolves which expectations of privacy are entitled to protection"); Thomas v. Cash, 423 P.3d 670, 676 n.8 (Okla. Civ. App. 2016) (noting that "[w]hether a party may legitimately have an expectation of privacy in his or her Facebook postings or other communications is a developing area of the law").

29. *See, e.g.*, *Carpenter*, 138 S. Ct. at 2265 (Gorsuch, J., dissenting) ("[W]e still don't even know what [*Katz*'s] 'reasonable expectation of privacy' test is."); see also Barry Friedman & Cynthia Benin Stein, *Redefining What's "Reasonable": The Protections for Policing*, 84 GEO. WASH. L. REV. 281, 284 (2016) (stating with respect to the *Katz* test, "[a]ll that the Supreme Court has provided by way of guidance is a growing litany of vague and indeterminate phrases and legal tests").

30. *See infra* Part I.

privacy settings. We also highlight the growing body of research showing a stark disconnect between users' privacy expectations and the behavior of firms in the online environment. Facebook, for instance, the world's most popular social media platform,[31] assures users that they "have control over who sees what [they] share on Facebook,"[32] and like other providers,[33] allows users to adjust privacy settings.[34] Yet service agreements frequently reserve to firms the right to monitor and disclose content, doing so in lengthy and often unreadable documents not subject to negotiation, in a manner often intentionally designed to mislead. Aggravating matters, the agreements change with regularity, and website and application designs obfuscate users' understandings of privacy.

Given the acknowledged problems with notice and consent, we maintain that ambiguity in agreements should generally be construed against the drafter and in favor of the user-consumer. When an ambiguity exists regarding whether a user is on notice of the waiver of privacy rights, or disclosure to third parties, the ambiguity should cut against waiver and in favor of users' privacy rights. Moreover, promises made by firms to protect privacy, whether by dint of agreement, behavior, or privacy settings, should be construed to preserve Fourth Amendment privacy.

Our discussion, which aligns with increasing recognition of the influence of private ordering on public law more generally,[35] provides the first in-depth analysis of how contract doctrine can be employed in Fourth Amendment analysis. As we note in Part IV, embracing this shift will have its challenges, but on balance,

31. *Most Famous Social Networks Worldwide as of July 2019, Ranked by Number of Active Users (in Millions)*, STATISTA, https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ [https://perma.cc/YQK2-QFU4].

32. *Privacy Basics*, FACEBOOK, https://www.facebook.com/about/basics [https://perma.cc/5DJ5-KSFU].

33. *See, e.g.*, *How to Protect Your Personal Information*, TWITTER, https://help.twitter.com/en/safety-and-security/twitter-privacy-settings [https://perma.cc/5DJ5-KSFU].

34. *Manage Your Privacy*, FACEBOOK, https://www.facebook.com/about/basics/manage-your-privacy [https://perma.cc/FRP2-9JY5].

35. *See, e.g.*, Lawrence A. Cunningham, *Private Standards in Public Law: Copyright, Lawmaking and the Case of Accounting*, 104 MICH. L. REV. 291 (2005); Alan Schwartz & Robert E. Scott, *The Political Economy of Private Legislatures*, 143 U. PA. L. REV. 595 (1995); Peter L. Strauss, *Private Standards Organizations and Public Law*, 22 WM. & MARY BILL RTS. J. 497, 498 (2013).

importing contract tools of interpretation holds significant promise for providing a reliable analytic rubric for resolving online privacy questions in the Internet Age.

I. REASONABLE EXPECTATIONS OF PRIVACY AND THE THIRD PARTY DOCTRINE

For better or worse, the courts have been charged with elucidating the Fourth Amendment's amorphous prohibition of "unreasonable searches and seizures."[36] Modern wisdom on the issue dates to the Supreme Court's seminal 1967 decision in *Katz v. United States*.[37] In *Katz*, police, acting without a search warrant, placed a listening device on the outside of a telephone booth and eavesdropped on the defendant's conversation, which implicated him in an illegal betting operation.[38] Had the Court elected to rely on its prior Prohibition Era decision in *Olmstead v. United States*,[39] the fact that police did not place the device inside the phone booth would have meant that they did not conduct a search and therefore did not need to obtain a warrant.[40]

The *Katz* majority, however, articulated a new definition of a search, one not dependent upon whether police engaged in a "physical penetration" of the space inhabited by the individual,[41] or the public nature of where the snooping occurred.[42] This was because

> the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[43]

Elaborating, Justice Stewart noted that Katz, who spoke from a telephone booth partially made of glass,[44] "sought to exclude . . . not the intruding eye—[but rather] the uninvited ear.

36. U.S. CONST. amend. IV.

37. 389 U.S. 347 (1967).

38. *Id.* at 348.

39. 277 U.S. 438 (1928), *overruled by Katz*, 389 U.S. at 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

40. *Katz*, 389 U.S. at 352–53 (citing *Olmstead*, 277 U.S. at 457, 464, 468).

41. *Id.* at 350.

42. *Id.* at 351.

43. *Id.* at 351–52 (citations omitted).

44. *Id.* at 352.

He did not shed his right to do so simply because he made his calls from a place where he might be seen."[45]

Concurring, Justice Harlan provided what has become the doctrinal takeaway of *Katz*: whether an expectation of privacy exists depends on first whether an individual "exhibited an actual (subjective) expectation of privacy" and then whether "the expectation [is] one that society is prepared to recognize as 'reasonable.'"[46] Under the test, even if a person might expect privacy—for instance in their home—the expectation can be lost because any "objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited."[47]

Despite its importance, *Katz* was not the Court's first foray into the issue of whether an individual enjoys privacy protection in their communications with others. In a series of decisions dating back to 1952, the Court held that individuals who confide information in others assume the risk of having their confidence betrayed, irrespective of whether the betrayer is actually a police informant[48] or an undercover police officer.[49] A year before *Katz*, the Court issued one of its most noteworthy decisions in this regard, holding that labor leader James Hoffa lacked an expectation of privacy in his conversation with an associate, who later briefed law enforcement on Hoffa's incriminating statements. The Court reasoned that Hoffa relied upon "his misplaced confidence that [the informant] would not reveal his wrongdoing."[50] Four years after *Katz*, in *United States v. White*,[51] the Court applied similar reasoning to uphold a conviction based upon statements made by a defendant to a government informant who was wearing a "wire."[52]

A few years later, the Court applied similar reasoning to records collected by or provided to and stored by third parties. First,

45. *Id.*

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

47. *Id.*

48. On Lee v. United States, 343 U.S. 747, 750–51 (1952).

49. Lewis v. United States, 385 U.S. 206, 210–11 (1966).

50. Hoffa v. United States, 385 U.S. 293, 302 (1966); *see also id.* (noting that the Court has never "expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it").

51. 401 U.S. 745 (1971).

52. *Id.* at 748–50.

in *United States v. Miller*,[53] the Court held that an individual lacked a reasonable expectation of privacy in financial records (such as personal checks and deposit slips) possessed by a bank where he did business.[54] This was because:

> [t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. 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.[55]

Next, in *Smith v. Maryland*,[56] the Court held that police did not invade a reasonable expectation of privacy when they secretly installed a "pen register" that enabled them to determine the telephone number of calls dialed on an individual's phone.[57] The Court distinguished the phone numbers dialed from the information obtained in a phone wiretap (the contents of a call), and held that Smith lacked a reasonable expectation of privacy in the numbers dialed.[58] The Court doubted "that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed."[59] In addition, at the time, phone users such as the defendant were reasonably on notice because phone companies then recorded outgoing calls for a variety of purposes, including long-distance billing and fraud and harassment detection.[60] Finally, to the extent a phone user had a contrary belief, the Court held that such a belief was unreasonable based on its prior misplaced trust decisions.[61]

The contours of the third party doctrine post-*Katz* seemed settled for a third of a century, affording courts a relatively clear-

53. 425 U.S. 435 (1976).

54. *Id.* at 442–43.

55. *Id.* (citations omitted).

56. 442 U.S. 735 (1979).

57. *Id.* at 735. *Smith* involved the rather curious case of an alleged robber who repeatedly phoned his victim and subjected her to obscene and harassing calls. Police, acting without a search warrant, installed and used the pen register information to secure an arrest warrant for the defendant. *Id.* at 737.

58. *Id.* at 741–42.

59. *Id.* at 742.

60. *Id.* at 742–43.

61. *Id.* at 743–45.

cut basis to restrict privacy rights when information is shared with another person or entity. The doctrine has survived despite continued criticism from commentators who question its basic assumptions, such as that one assumes the risk that a confidant will disclose shared information with the police.[62] Indeed, as the Sixth Circuit Court of Appeals noted in *United States v. Warshak*:[63] "In *Katz*, the Supreme Court found it reasonable to expect privacy during a telephone call despite the ability of an operator [at that time] to listen in."[64] Thus, following *Katz*, "the threat or possibility of access is not decisive when it comes to the reasonableness of an expectation of privacy."[65] And even if one subscribes to the view that the digits in the telephone numbers discovered by police in *Smith* were not deserving of privacy protection, one need not—as indeed the Court in *Smith* did not[66]—conclude that the content of the phone conversations themselves lacked privacy protection. At the same time, as critics have pointed out, the third party doctrine is ill-suited to the evolving interconnected world where so much interaction and expression occurs online, posing distinct chilling concerns with respect to First Amendment freedom of expression and association.[67]

62. As Richard Epstein has noted, we engage in a "false equation" when we blur knowledge of a risk with the assumption of a risk. Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 BERKELEY TECH. L.J. 1199, 1204 (2009) ("The acceptance of a risk does not follow from knowledge of the risk . . . . Each day I walk down the street I know that some automobile may hurt me. Yet I do not assume the risk of which I am fully aware."); *see also Smith*, 442 U.S. at 749 (Marshall, J., dissenting) ("Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes.").

63. 631 F.3d 266 (6th Cir. 2010).

64. *Id.* at 287 (citing *Smith*, 442 U.S. at 746–47 (Stewart, J., dissenting)).

65. *Id.*; *see also* Rubenfeld, *supra* note 9, at 115 (asserting that under the third party doctrine "the Fourth Amendment ends up a hollow shell, because in an increasingly digitized, networked world with ever-expanding privacy-invading technologies, virtually all information is exposed to third parties. Even *Katz* had exposed the seized information to a third party; hence *Katz* itself becomes inexplicable").

66. *Smith*, 442 U.S. at 741.

67. *See, e.g.*, Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441, 1442–48 (2010); Jonathon W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERKELEY TECH. L.J. 117, 122 (2016); Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 143–44 (2007).

In *United States v. Jones*,[68] decided in 2012, Justice Sotomayor identified and expounded upon many of these concerns. In *Jones*, police attached a Global Positioning System tracking device to a car Jones drove for approximately a month and used this aggregated geo-locational information to deduce that Jones was involved in drug trafficking.[69] Justice Scalia's majority opinion, with which Justice Sotomayor concurred providing the dispositive fifth vote, rejuvenated physical trespass theory by concluding that a search occurred when police attached the device to the car and used the information they obtained for investigative purposes.[70]

Justice Sotomayor agreed that the case could be decided on trespass grounds.[71] However, she wrote at length about the privacy implications of locational surveillance technology, in particular the sensitive personal information that analysis of the metadata might reveal.[72] In addition to waxing eloquent about the broader negative societal implications of extended locational surveillance by the government,[73] Justice Sotomayor questioned the premise that "an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill-suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[74] Justice Sotomayor thus declined to assume "that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."[75]

68. 565 U.S. 400 (2012).

69. *Id.* at 403.

70. *Id.* at 406–12.

71. *Id.* at 413–14 (Sotomayor, J., concurring).

72. *See id.* at 415 ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.").

73. *See id.* at 416 ("[T]he Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may alter the relationship between citizen and government in a way that is inimical to democratic society." (citation omitted)).

74. *Id.* at 417 (citation omitted).

75. *Id.* at 418. Justice Alito also wrote a concurrence, joined by the other three Justices, resulting in a unanimous determination by the Court that a

In its most recent decision regarding geo-locational metadata, *Carpenter v. United States*,[76] the Court refused to directly address the continued viability of the third party doctrine,[77] yet signaled its less than full-throated endorsement.[78] In *Carpenter*, the Court considered whether collection of cell site location information (CSLI), generated when a defendant's cell phone connected to cell towers and detailed his public travel, qualified as a search.[79]

Disagreeing with the Sixth Circuit, the Court held that a search occurred, requiring that police secure a warrant based on probable cause of wrongdoing, rather than the lower standard ("reasonable grounds") required for obtaining a court order under the federal Stored Communications Act.[80] The five-member majority opinion, authored by Chief Justice Roberts, recognized the third party doctrine's application to "telephone numbers and bank records" but declined to extend "its logic" to "the qualitatively different category" of CSLI.[81] The Court concluded that like the GPS information in *Jones*, CSLI records "provide[] an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[82]

Fourth Amendment search occurred. *Id.* at 418 (Alito, Ginsburg, Breyer & Kagan, JJ., concurring). Justice Alito opined that the case should be resolved on the basis of the *Katz* reasonable expectation of privacy test. *Id.* at 419. He reasoned that while "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable . . . the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." *Id.* at 430.

76. 138 S. Ct. 2206 (2018).

77. *Id.* at 2220 ("We do not express a view on matters not before us . . . . We do not disturb the application of *Smith* and *Miller*, or call into question conventional surveillance techniques and tools, such as security cameras.").

78. *Id.*

79. *Id.* at 2211–21.

80. *Id.* at 2221–22.

81. *Id.* at 2216–17; *see also id.* at 2217 ("After all, when *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements."); *id.* at 2219 ("There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today. The Government thus is not asking for a straightforward application of the third-party doctrine, but instead a significant extension of it to a distinct category of information.").

82. *Id.* at 2217 (quoting United States v. Jones, 565 U.S. 400, 415 (2012)).

Perhaps more importantly, the majority elaborated on what it saw as the foundations of the third party doctrine. The doctrine only "partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another."[83] *Miller* and *Smith*, the majority reasoned, "considered 'the nature of the particular documents sought'" in assessing whether the parties had a reasonable expectation of privacy.[84] The telephone numbers in *Smith* revealed "little in the way of 'identifying information,'"[85] and the bank records in *Miller* were not of a confidential nature.[86] Cautioning against "mechanically applying" the doctrine, the majority emphasized the "revealing nature of CSLI," which provided "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years. Such a chronicle implicates privacy concerns far beyond those considered in *Smith* and *Miller*."[87]

The majority also distinguished CSLI based on the "second rationale underlying the third party doctrine—voluntary exposure."[88] CSLI "is not truly 'shared' as one normally understands the term."[89] Carrying and use of a cell phone is "indispensable to participation in modern society."[90] Moreover, the tracking function of cell phones does not require

> any affirmative act on the part of the user beyond powering up . . . . Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements.[91]

Dissenting, Justice Kennedy, joined by Justices Thomas and Alito,[92] concluded that *Carpenter* neither created nor owned the CSLI information, and reasoned that therefore *Smith* and *Miller* controlled.[93] The dissent added, however, that "[a]ll this is not to

83. *Id.* at 2219.

84. *Id.* (quoting United States v. Miller, 425 U.S 435, 442 (1976)).

85. *Id.* (quoting Smith v. Maryland, 442 U.S. 735, 742 (1979)).

86. *Id.* (citing *Smith*, 442 U.S. at 742; Riley v. California, 134 S. Ct. 2473, 2493 (2014); *Miller*, 425 U.S. at 442).

87. *Id.* at 2219–20.

88. *Id.* at 2220.

89. *Id.*

90. *Id.* (citing *Riley*, 134 S. Ct. at 2484).

91. *Id.* (quoting *Smith*, 442 U.S. at 745).

92. *Id.* at 2223 (Kennedy, Thomas, & Alito, JJ., dissenting).

93. *Id.* at 2230 ("Because Carpenter lacks a requisite connection to the cell-site records, he also may not claim a reasonable expectation of privacy in them. He could expect that a third party—the cell phone service provider—could use

say that *Miller* and *Smith* are without limits. *Miller* and *Smith* may not apply when the Government obtains the modern-day equivalents of an individual's own 'papers' or 'effects,' even when those papers or effects are held by a third party."[94]

Justice Kennedy accused the majority of "misinterpreting"[95] and "reinterpret[ing]"[96] *Miller* and *Smith*. The majority, he contended, "establish[ed] a balancing test."[97] For each "qualitatively different category of information . . . the privacy interests at stake must be weighed against the fact that the information has been disclosed to a third party. When the privacy interests are weighty enough to 'overcome' the third party disclosure, the Fourth Amendment's protections apply."[98] The dissent termed the foregoing as "an untenable reading of *Miller* and *Smith*," cases where "the fact that information was relinquished to a third party was the entire basis for concluding that the defendants in those cases lacked a reasonable expectation of privacy."[99]

Justice Thomas filed an individual dissent, urging the Court to repudiate the reasonable expectation of privacy test formulated in *Katz*.[100] Justice Alito, joined by Justice Thomas, also dissented,[101] asserting that the process outlined by Congress in the Stored Communications Act afforded all the protection needed to secure the CSLI records, that the defendant enjoyed no property interest in the records, and that the Fourth Amendment therefore did not govern.[102]

Justice Gorsuch, in yet another dissent,[103] similarly condemned *Katz* as lacking a constitutional basis,[104] but also criticized at length the third party doctrine.[105] To Justice Gorsuch,

---

the information it collected, stored, and classified as its own for a variety of business and commercial purposes.").

94. *Id.* (citing *Ex parte* Jackson, 96 U.S. 727, 733 (1878); *Warshak III*, 631 F.3d 266, 283–88 (6th Cir. 2010)).

95. *Id.* at 2231.

96. *Id.* at 2233.

97. *Id.* at 2231.

98. *Id.* at 2231–32 (internal quotations and citations omitted).

99. *Id.* at 2232.

100. *Id.* at 2235–36 (Thomas, J., dissenting).

101. *Id.* at 2246 (Alito & Thomas, JJ., dissenting).

102. *Id.* at 2255.

103. *Id.* at 2261 (Gorsuch, J., dissenting).

104. *Id.* at 2264–68.

105. *See, e.g.*, *id.* at 2263–64 ("Consenting to give a third-party access to private papers that remain my property is not the same thing as consenting to a

the view that information loses its privacy protection simply because it comes into the possession of a third party is belied by reason and experience:

> People often do reasonably expect that information they entrust to third parties, especially information subject to confidentiality agreements, will be kept private. Meanwhile, if the third party doctrine is supposed to represent a normative assessment of when a person should expect privacy, the notion that the answer might be "never" seems a pretty unattractive societal prescription.[106]

Nor, he maintained, do individuals assume the risk that their information will be provided to police when they share it with a third party.[107] Assumption of risk arose in tort law and "generally applies when 'by contract or otherwise [one] expressly agrees to accept a risk of harm' or impliedly does so by 'manifest[ing] his willingness to accept' that risk and thereby 'take[s] his chances as to harm which may result from it.'"[108] The rationale, Justice Gorsuch reasoned, "has little play in this context," and offered the following hypothetical:

> Suppose I entrust a friend with a letter and he promises to keep it secret until he delivers it to an intended recipient. In what sense have I agreed to bear the risk that he will turn around, break his promise, and spill its contents to someone else? More confusing still, what have I done to "manifest my willingness to accept" the risk that the government will pry the document from my friend and read it *without* his consent?[109]

Justice Gorsuch offered that one answer might lie in knowledge of the potentiality that the promise could be broken or that the government might search the friend.[110] "But knowing about a risk doesn't mean you assume responsibility for it. Whenever you walk down the sidewalk you know a car may negligently or recklessly veer off and hit you, but that hardly means you accept the consequences and absolve the driver of any damage he may do to you."[111]

Nor, Justice Gorsuch reasoned, does the third party doctrine rest on consent:

> Consenting to give a third party access to private papers that remain my property is not the same thing as consenting to a *search of those*

search of those papers by the government."); *id*. at 2264 ("Clarity alone cannot justify the third-party doctrine.").

106. *Id*. at 2263 (citation omitted).

107. *Id*.

108. *Id*. (alterations in original) (citations omitted).

109. *Id*.

110. *Id*.

111. *Id*. (citations omitted).

> *papers by the government*. Perhaps there are exceptions, like when the third party is an undercover government agent . . . . But otherwise this conception of consent appears to be just assumption of risk relabeled—you've "consented" to whatever risks are foreseeable.[112]

Justice Gorsuch also rejected the contention that a commitment to clarity supported continued fealty to the third party doctrine:

> As rules go, "the king always wins" is admirably clear. But the opposite rule would be clear too: Third party disclosures never diminish Fourth Amendment protection (call it "the king always loses"). So clarity alone cannot justify the third party doctrine.
>
> In the end, what do Smith and Miller add up to? A doubtful application of Katz that lets the government search almost whatever it wants whenever it wants.[113]

Finally, like Justice Kennedy, Justice Gorsuch detected in the majority's approach an apparent shift in third party doctrine, writing that "apparently *Smith* and *Miller* aren't quite left for dead; they just no longer have the clear reach they once did."[114] Gorsuch condemned what he saw as the indeterminacy of the majority's test, writing that "[a]ll we know is that historical cell-site location information (for seven days, anyway) escapes *Smith* and *Miller*'s shorn grasp, while a lifetime of bank or phone records does not. As to any other kind of information, lower courts will have to stay tuned."[115]

Justice Gorsuch concluded by offering an alternative approach, one based on "ancient principles" sounding in property. He reasoned that the privacy interest in modern day "papers and effects"—data—should not be categorically surrendered when shared with a third party.[116] "Whatever may be left of *Smith* and *Miller*," Gorsuch wrote, "few doubt that e-mail should be treated much like the traditional mail it has largely supplanted—as a bailment in which the owner retains a vital and protected legal interest."[117] For Justice Gorsuch, the proper rule would hold, at a minimum, that "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."[118]

112. *Id.* at 2263.
113. *Id.* at 2264.
114. *Id.* at 2267.
115. *Id.*
116. *Id.* at 2269.
117. *Id.*
118. *Id.* at 2270.

II. THE THIRD PARTY DOCTRINE AND THE EMERGENCE OF CONTRACT LAW METHODOLOGY

As noted earlier, law enforcement in recent years has increasingly availed itself of information shared by individuals engaged in the online environment. The third party doctrine, strictly applied, would render such information fair game for police use, as the act of sharing with another would itself negate any reasonable expectation of privacy. A review of the emerging case law, however, reveals that courts often eschew strict application of the doctrine, and resolve privacy questions by assessing users' privacy settings, content of terms of service agreements, and the like.

A. PRIVACY SETTINGS

At the outset, it must be acknowledged that courts most often conclude that individuals lack a privacy right in their online information and communications. Assumption of risk is a common supporting rationale of such courts.[119] For instance, in *Everett v. State*,[120] the Supreme Court of Delaware held that the defendant lacked an expectation of privacy because his Facebook "friends" setting allowed an officer to become a "false friend."[121] The defendant made an incriminating Facebook photo "accessible to his 'friends' and, by doing so, he assumed the risk that one of them might be a government officer or share his information with law enforcement."[122] Some courts so conclude even if users have attempted to preserve privacy by adjusting available settings. For instance, in *Nucci v. Target Corp.*,[123] an appellate state court in Florida held in a tort case that "photographs posted on a social networking site are neither privileged nor protected by

119. *See, e.g.*, Palmieri v. United States, 72 F. Supp. 3d 191, 210 (D.D.C. 2014) ("[W]hen a Facebook user allows 'friends' to view his information, the Government may access that information through an individual who is a 'friend' without violating the Fourth Amendment."); Rosario v. Clark Cty. Sch. Dist., No. 2:13–CV–362 JCM (PAL), 2013 WL 3679375, at *6 (D. Nev. July 3, 2013) ("When a person tweets on Twitter to his or her friends, that person takes the risk that the friend will turn the information over to the government."); United States v. Meregildo, 883 F. Supp. 2d 523, 526 (S.D.N.Y. 2012) ("Where Facebook privacy settings allow viewership of postings by 'friends,' the Government may access them through a cooperating witness who is a 'friend' without violating the Fourth Amendment.").

120. 186 A.3d 1224 (Del. 2017).

121. *Id.* at 1231.

122. *Id.* at 1229.

123. 162 So. 3d 146 (Fla. Dist. Ct. App. 2015).

any right of privacy, regardless of any privacy settings that the user may have established."[124]

Other courts, however, recognize the range of privacy preferences available to users[125] and acknowledge the importance of privacy setting designations in assessing whether users have waived privacy protections or assumed the risk of subsequent dissemination.[126] In a leading case on the issue, *United States v. Meregildo*,[127] the Southern District of New York noted that whether a user has a privacy right "depends, *inter alia*, on the user's privacy settings," and that "postings using more secure privacy settings reflect the user's intent to preserve information as private and may [therefore] be constitutionally protected."[128] Although the court ultimately concluded that the defendant lacked a reasonable expectation of privacy when police gained access to incriminating information on his Facebook profile via one of his "friends," a cooperating witness, the court qualified its reasoning. Citing *Katz*, it recognized that "[w]hen a social media user disseminates his postings and information to the public, they are not protected by the Fourth Amendment . . . . However, postings using more secure privacy settings reflect the user's intent to preserve information as private and may be constitutionally protected."[129]

124. *Id.* at 153.

125. *See, e.g.*, United States v. Westley, No. 3:17-CR-171 (MPS), 2018 WL 3448161, at *6 (D. Conn. July 17, 2018) (acknowledging that "[t]here is a spectrum of privacy settings available on Facebook, and those settings can be tailored to specific types of communications").

126. *See, e.g.*, United States v. Khan, Case No. 15-cr-00286, 2017 WL 2362572, at *8 (N.D. Ill. May 31, 2017) ("Defendant did not maintain any privacy restrictions on his Facebook account, and his Facebook profile was viewable by any Facebook user. Hence, Defendant possessed no reasonable privacy expectation in the information found on his Facebook page. As a result, he cannot claim a Fourth Amendment violation."); United States v. Adkinson, Case No. 4:15-cr-00025-TWP-VTW, 2017 WL 1318420, at *5 (S.D. Ind. Apr. 7, 2017) ("There is no expectation of privacy in an open Facebook page."); *see also, e.g.*, Chaney v. Fayette Cty. Pub. Sch. Dist., 977 F. Supp. 2d 1308, 1316 (N.D. Ga. 2013); United States v. Meregildo, 883 F. Supp. 2d 523, 525 (S.D.N.Y. 2012); United States v. Devers, Case No. 12-CR-50-JHP, 2012 WL 12540235, at *2–3 (N.D. Okla. Dec. 28, 2012).

127. 883 F. Supp. 2d 523, 525 (S.D.N.Y. 2012).

128. *Id.*

129. *Id.* (citing Katz v. United States, 389 U.S. 347, 351–52 (1967)). Here, the court likely meant dissemination to the "public at large," used in Facebook's terms of service, as distinguishable from information shared "only with 'friends' or more expansively with 'friends of friends.'" *Id.* (quoting *Facebook Help Center*,

Likewise, in *United States v. Devers*,[130] the Northern District of Oklahoma held that:

> [U]nless the defendants can prove that their [F]acebook accounts contained security settings which prevented anyone from accessing their accounts, . . . their legitimate expectation of privacy ended when they disseminated posts to their "friends" because those "friends" were free to use the information however they wanted—including sharing it with the government.[131]

Similarly, in *Chaney v. Fayette County Public School District*, a high school student sued a local school district for making publicly available a photo of her in a bikini swimsuit to highlight the dangers of social media.[132] The Northern District of Georgia held that the plaintiff lacked an expectation of privacy because:

> She shared her Facebook page, which includes her pictures, not only with her friends but their friends, too. By doing so, [the plaintiff] surrendered any reasonable expectation of privacy when she posted a picture to her Facebook profile, which she chose to share with the broadest audience available to her.[133]

Many other cases are in accord.[134]

Facebook, http://www.facebook.com/help/privacy [https://perma.cc/N2Q4-6B7V]).

130. 2012 WL 12540235, at *2.

131. *Id.*

132. Chaney v. Fayette Cty. Pub. Sch. Dist., 977 F. Supp. 2d 1308 (N.D. Ga. 2013).

133. *Id.* at 1316; *see also, e.g.*, United States v. Jordan, No. 16-CR-93-G, 2017 WL 9516819, at *8 (W.D.N.Y. July 14, 2017). In *Jordan*, the court explained:

> In the context of Facebook, a person who allows a wide circle of 'friends' to access his profile does not have a reasonable expectation of privacy. This is because once a user disseminates a post to his "friends," those 'friends,' being under no obligation to keep his profile private, are free to share that information anyway they like . . . .
>
> Jordan testified at the grand jury that he did not know many of his Facebook 'friends,' but accepted their requests because he '[m]ight get to know them.' This Court finds it patently unreasonable that Jordan would have any expectation of privacy in a post published to this expansive circle of near strangers.

Id. (citations omitted).

134. *See, e.g.*, United States v. Westley, No. 3:17-CR-171 (MPS), 2018 WL 3448161, at *6 (D. Conn. July 17, 2018) (noting that because the defendants did "nothing to show what, if any, privacy settings governed any of the types of communications found in their accounts," they failed to establish that they had a reasonable expectation of privacy "in any of the communications" distributed through the accounts); United States v. Khan, No. 15-cr-00286, 2017 WL 2362572, at *8 (N.D. Ill. May 31, 2018) ("Here, at the time of Special Agent Walther's viewing, Defendant did not maintain any privacy restrictions on his Facebook account, and his Facebook profile was viewable by any Facebook user.

Privacy settings are also at issue in cases construing the Stored Communications Act (SCA).[135] A key question in such cases is when an individual provides "lawful consent" sufficient to allow a provider to voluntarily disclose a communication,[136] which courts have concluded turns on the privacy preference of the individual. The California Supreme Court recently addressed this question in *Facebook, Inc. v. Superior Court*.[137] There, defendants in a homicide case subpoenaed Facebook, Instagram, and Twitter to obtain communications from social media accounts belonging to the victim and a prosecution witness. The social media providers sought to quash the subpoenas.[138]

The court in *Facebook* unanimously held that while unrestricted public disseminations are subject to the SCA exception,[139] "restricted communications sent to numerous recipients cannot be deemed to be public—and do not fall within the lawful consent exception."[140] The court backed its conclusion by considering the SCA's legislative history, which suggested "that Congress intended to exclude from the scope of the lawful consent exception communications configured by the user to be accessible to only specified recipients."[141] This was so even if there are "a large number of recipients" and even if they "could have shared such communications with others who were not intended by the original poster to be recipients."[142]

The court noted that the House Judiciary Committee, for its part, believed that "a user's configuration would 'establish an objective standard'" for evaluating consent and "that a user's consent to disclosure could be implied in view of, among other things, providers' available published policies."[143] Concluding, the court stated:

> [N]othing of which we are aware in any of providers' policies or answers to FAQs suggests that users would have any reason to expect that, having configured a communication to be available not to the public but

Hence, Defendant possessed no reasonable privacy expectation in the information found on his Facebook page. As a result, he cannot claim a Fourth Amendment violation.").

135. 18 U.S.C. §§ 2701–12 (2018).
136. *See id.* § 2702(b)(3).
137. 417 P.3d 725 (Cal. 2018).
138. *Id.* at 727–28.
139. *Id.* at 728.
140. *Id.*
141. *Id.* at 747.
142. *Id.*
143. *Id.* at 748.

> instead to a restricted group of friends or followers, the user nevertheless has made a *public* communication—and hence has impliedly consented to disclosure by a service provider, just as if the configuration had been public.
>
> For all of these reasons we reject defendants' proposed broad interpretation of the lawful consent exception. We hold that implied consent to disclosure by a provider is not established merely because a communication was configured by the user to be accessible to a "large group" of friends or followers.[144]

The District of New Jersey held likewise in *Ehling v. Monmouth-Ocean Hospital Service Corp.*[145] In *Ehling*, the court concluded that privacy rights turned on whether an individual "actively restrict[ed] the public from accessing information."[146] Where the user configures a communication to be available on only a limited basis and it is "inaccessible to the general public," the communication is "'configured to be private' for purposes of the SCA."[147] Elaborating, the *Ehling* court stated:

> [W]hen users make their Facebook wall posts inaccessible to the general public, the wall posts are "configured to be private" for purposes of the SCA . . . [W]hen it comes to privacy protection, the critical inquiry is whether Facebook users took steps to limit access to the information on their Facebook walls. Privacy protection provided by the SCA does not depend on the number of Facebook friends that a user has. "Indeed, basing a rule on the number of users who can access information would result in arbitrary line-drawing" and would be legally unworkable.[148]

It is worth noting that the SCA's lawful consent exception, construed in *Facebook* and *Ehling*, arguably utilizes a more restrictive consent standard than that operative with traditional third party doctrine. Under the SCA, disclosure of "stored communications" is prohibited by law unless an exception like lawful consent permits the disclosure, and courts conclude that the

144. *Id.* at 748–49 (footnotes and citations omitted).

145. 961 F. Supp. 2d 659, 661 (D.N.J. 2013); *see also* Snow v. DirectTV, Inc., 450 F.3d 1314, 1321 (11th Cir. 2006) (noting that an "express warning, on an otherwise publicly accessible webpage," was insufficient to avoid negating SCA protection); Burke v. New Mexico, No. 16-cv-0470 MCA/SMV, 2018 WL 3054674 (D.N.M. June 20, 2018) (holding that a failure to designate privacy settings when posting medical information on CaringBridge negated SCA privacy protection); accord Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010).

146. *Ehling*, 961 F. Supp. 2d at 668.

147. *Id.*

148. *Id.* (citations omitted).

originator does not consent unless the communications are accessible to the general public.[149] Use of a restrictive configuration is sufficient to avoid implied consent to disclosure, even if the closed list of potential recipients is a "'large group' of friends or followers."[150] Under a traditional reading of the third party doctrine, on the other hand, any disclosure to a third party negates a privacy expectation.[151]

One might conclude these differing standards limit the relevance of the SCA cases. But the foregoing SCA cases share critical analytic features with non-SCA cases. In both lines of cases, courts properly consider users' manipulation of privacy preferences in determining whether they retain a reasonable expectation of privacy, despite sharing information with others. For reasons we detail in Part III, the SCA cases better reflect users' reasonable expectations vis-à-vis privacy preferences they select online.

B. TERMS OF SERVICE AGREEMENTS

Courts also employ contractual tools of analysis to determine privacy interests established or waived by standard form terms of service agreements and privacy policies. These terms, typically drafted by providers, are not always presented to users for affirmative acceptance and are frequently modified after the fact. As we will discuss, there is scant reason to believe that users read or understand these terms.

Perhaps the leading case in this regard is *United States v. DiTomasso*.[152] In *DiTomasso*, law enforcement, acting without a search warrant, obtained two forms of evidence: (1) emails, after examination by the defendant's Internet service provider (ISP), America Online (AOL); and (2) "chats," after examination by another ISP, Omegle.com LLC.[153]

In assessing the defendant's privacy claim, Judge Scheindlin, of the Southern District of New York, concluded as a threshold matter that defendant's mere sharing of information

149. *See, e.g.*, Facebook Inc. v. Super. Ct., 417 P.3d 725, 744 (Cal. 2018).
150. *Id.* at 749.
151. *See supra* Part I.
152. 56 F. Supp. 3d 584 (S.D.N.Y. 2014).
153. *Id.* at 586.

with another, by email (AOL) or chat (Omegle.com), did not relinquish his expectation of privacy.[154] The mere risk that a communication would be shared with law enforcement did not defeat a privacy expectation, she reasoned, because if this were the case any communication with another would be fair game for government eavesdropping, which *Katz* expressly rejected.[155] The court also rejected the government's argument that even if the emails were private, the chats were not because they were communicated in a forum akin to a "town square."[156] This was because rather than being available to the public at-large, the chat room "allow[ed] two strangers to chat anonymously, and only with one another."[157] Like emails and phone calls, each "involve[d] one-on-one interactions that users clearly expect to be kept private."[158]

Judge Scheindlin next addressed the privacy implications of the terms of service agreements used by the respective ISPs. The AOL agreement forbade posting of unlawful content; reserved to AOL the right to take action, including "'cooperat[ing] with law enforcement'"; and allowed AOL to disclose to others—including law enforcement—information "'relevant to a crime that has been or is being committed.'"[159] The agreement used by Omegle.com—an online platform that randomly pairs users in a "'one-on-one session with a stranger, and allows strangers to communicate via text and video chats'"[160]—provided that it would keep "'record[s] of the IP addresses involved in every chat,'" for reasons including "'for the purpose of law enforcement.'"[161] The policy also stated that Omegle would monitor content for "'quality control purposes,'" to help improve "'anti-spam software'" and monitor content on an ad hoc basis "'for misbehavior.'"[162] Finally, the Omegle policy warned users to be "'careful about what information [they] reveal'" during chats, because

154. *Id.* at 591.

155. *Id.* at 591–92.

156. *Id.* at 592.

157. *Id.*

158. *Id.*

159. *Id.* at 588 (quoting agreement).

160. *Id.* (quoting Declaration of Lief Brooks, Founder of Omegle.com).

161. *Id.* (quoting *Privacy Policy*, OMEGLE (June 3, 2019), https://www.omegle.com/static/privacy.html [https://perma.cc/6YCT-YWX9]).

162. *Id.*

"'strangers can potentially tell other people anything you tell them.'"[163]

Judge Scheindlin rejected the government's contention that because the ISPs warned that they might monitor activity the defendant lacked a privacy expectation in his communications. To Judge Scheindlin, waiver in such a circumstance "would subvert the purpose of the Fourth Amendment."[164] This was because

> [i]n today's world, meaningful participation in social and professional life requires using electronic devices—and the use of electronic devices almost always requires acquiescence to some manner of consent-to-search terms. If this acquiescence were enough to waive one's expectation of privacy, the result would either be (1) the chilling of social interaction or (2) the evisceration of the Fourth Amendment. Neither result is acceptable.[165]

Judge Scheindlin emphasized that privacy analysis raises a "context-sensitive question of societal norms."[166] Thus, "[i]n some domains, people expect information to stay shielded from law enforcement even as they knowingly disclose it to other parties. As the Supreme Court has recognized, workplace desks and hotel rooms are two such domains. In the digital age, electronic communication is another."[167]

The question, Judge Scheindlin reasoned, was to be determined "'objective[ly]'—by reference to what a 'typical reasonable person [would understand]' AOL's and Omegle's policies to mean."[168] The defendant would lack a privacy expectation only if he "contemplated a search by AOL or Omegle in a *law enforcement* capacity."[169]

Objectively viewed, the defendant's agreement with Omegle did not qualify as consent to search. The policy only provided a

163. *Id.* at 589.

164. *Id.* at 592.

165. *Id.*

166. *Id.* at 593.

167. *Id.* at 594 (citing O'Connor v. Ortega, 480 U.S. 709, 717–18 (1987); Stoner v. California, 376 U.S. 483, 84 (1964)); *cf.* Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611, 629–33 (2015) (arguing that entities such as hotel managers and ISPs are "Fourth Amendment fiduciaries" and that information disclosed to them should retain a reasonable expectation of privacy).

168. *DiTomasso*, 56 F. Supp. 3d at 596 (quoting Florida v. Jimeno, 500 U.S. 248, 250 (1991) (alterations in original)).

169. *Id.* ("[T]he policies only defeat [defendant's] constitutional claim if, by agreeing to them, he was consenting to a search by AOL and Omegle as government agents.").

basis for a reasonable person to conclude that by using the Omegle chat service

> he was running the risk that another party—including Omegle—might divulge his sensitive information to law enforcement. But this does not mean that a reasonable person would also think that he was consenting to let Omegle freely monitor his chats if Omegle was working *as an agent* of law enforcement.[170]

Following this construction, "a reasonable user would be unlikely to conclude that Omegle intended to act as an agent of law enforcement. And such a user would be even *less* likely to conclude that he had agreed to permit such conduct."[171]

The court reached a different conclusion with regard to the AOL policy. Unlike Omegle, AOL expressly warned users that it "reserve[d] the right to take any action it deems warranted . . . including cooperat[ing] with law enforcement . . . [and] reserve[d] the right to reveal to law enforcement information" about criminal activity.[172] Unlike Omegle's policy, AOL's policy made "clear that AOL intend[ed] to actively assist law enforcement."[173] The court concluded that "a reasonable person familiar with AOL's policy would understand that by agreeing to the policy, he was consenting not just to monitoring by AOL as an ISP, but also to monitoring by AOL as a government agent."[174]

Other courts have employed similar analysis to find that language in user agreements did not waive a privacy interest. In *United States v. Heleniak*,[175] the Western District of New York had before it the same AOL policy analyzed in *DiTomasso*, but concluded that issues of fact remained concerning whether the "defendant was familiar with AOL's policy to make his use of the service consent to search by a Government agent."[176] Furthermore, even if the defendant consented to AOL's viewing of materials and cooperation with the government, the court stated that it did not necessarily mean that it consented to a search by a third party, the National Center for Missing and Exploited Children, and "reference of his e-mails to another government (here,

170. *Id.* at 597.

171. *Id.*

172. *Id.* (internal quotation omitted) (discussing the active AOL Privacy Policy).

173. *Id.*

174. *Id.*; *cf.* United States v. Hart, No. 08-109-C, 2009 WL 2552347, at *25 (W.D. Ky. Aug. 17, 2009) (finding the plaintiff's expectation of privacy destroyed by the terms of Yahoo!'s privacy policy).

175. No. 14CR42A, 2015 WL 521287, *4–7 (W.D.N.Y. Feb. 9, 2015).

176. *Id.* at *7.

referral to the New York State Attorney General)."[177] Whether the defendant consented raised a question of fact to be resolved in an evidentiary hearing.[178]

Similarly, in *United States v. Warshak*,[179] the Sixth Circuit Court of Appeals addressed whether an individual possessed a reasonable expectation of privacy in the content of his emails. The *Warshak* court looked to the subscriber agreement between the user and the ISP, and found an expectation of privacy existed because the ISP's subscriber agreement only "indicat[ed] that [the ISP] *may* access and use [emails]," which did not negate the user's reasonable expectation of privacy in the emails.[180] The defendant retained a reasonable expectation of privacy in his emails because the terms of service did not disclose that the ISP would "'audit, inspect, and monitor' its subscriber's emails."[181]

Courts also can have qualms about agreements that they consider unclear vis-à-vis whether the provider would share content with law enforcement. In one New York state case, *People v. Pierre*,[182] the court wrote:

> It is not clear exactly what Google users were agreeing to by accepting the [T]erms of [S]ervice, because its language was vague. Significantly, Google's warning that it might review content is qualified by the rest of that sentence and the one that follows: "We may review content to determine whether it is illegal or violates our policies, and *we may remove or refuse to display content* we reasonably believe violates our policies or the law. *But that does not necessarily mean that we review content, so please don't assume that we do*."183

The court then considered what would happen if Google reviewed content and concluded it was improper. Construing the

177. *Id.*

178. *Id.*

179. *Warshak III*, 631 F.3d 266 (6th Cir. 2010).

180. *Id.* at 287. However, the Sixth Circuit warned that "a subscriber agreement might, in some cases, be sweeping enough to defeat a reasonable expectation of privacy in the contents of an email account." *Id.* at 286. As an example, it offered that "if the ISP expresses an intention to 'audit, inspect, and monitor' its subscriber's emails, that might be enough to render an expectation of privacy unreasonable." *Id.* at 287.

181. *Id.*; *see also, e.g.*, United States v. Maxwell, 45 M.J. 406, 417 (C.A.A.F. 1996) (noting that defendant had a reasonable expectation of privacy in information stored at America Online's computer center, in part because "AOL's contractual obligations with appellant insured him privacy"); Negro v. Superior Court, 179 Cal. Rptr. 3d 215, 234 (Cal. Ct. App. 2014) (explaining that information an ISP must be required to disclose pursuant to the Stored Communication Act "can go no farther than the consent" given by the user).

182. 29 N.Y.S. 3d 110 (N.Y. Sup. Ct. 2016).

183. *Id.* at 114–15.

agreement, the court noted two consequences: removal of objectionable material and a block on its display.[184] "There is no reference of any kind to law enforcement, much less an indication that Google intended to cooperate with law enforcement entities by turning over such material to them."[185] Therefore, the court concluded "while it could be fairly inferred that Google users were consenting to monitoring by the company for compliance with its policies, it cannot be fairly inferred that users were consenting to a search so as to defeat a Fourth Amendment claim about the nature of waiver."[186]

Finally, *United States v. Adkinson*[187] exemplifies how an express acknowledgement that an ISP might share data can defeat a privacy claim. In *Adkinson*, the Northern District of Indiana held (pre-*Carpenter*) that a defendant lacked privacy in his cellphone locational data when his cell provider's privacy policy established that it may "disclose, without . . . consent, the approximate location of a wireless device to a governmental entity or law enforcement authority when . . . [it] reasonably believe[s] there is an emergency involving risk of death or serious physical harm."[188]

C. SUMMARY

Taken together, the cases discussed above offer some intriguing insights into the ways in which courts are assessing Fourth Amendment privacy rights in the Internet Age. With privacy settings, many courts hold that it is not enough that one or more other individuals have access to a user's information. Rather, eschewing mechanical application of the third party doctrine, they look to whether users have designated their settings as "private." When users do so, courts often attach importance to

184. *Id.*

185. *Id.* at 115.

186. *Id.*; *see also, e.g.*, Lukowski v. Cty. of Seneca, No. 08-CV-6098, 2009 WL 467075, at *10 (W.D.N.Y. Feb. 24, 2009) (noting that while users may have a subjective expectation of privacy, the terms of the service agreement are relevant to determine the objective expectation of privacy).

187. Case No. 4:15-cr-00025-TWP-VTW, 2017 WL 1318420, at *4 (S.D. Ind. Apr. 7, 2017), *aff'd*, 916 F.3d 605 (7th Cir. 2019).

188. *Id.* The Seventh Circuit on appeal upheld denial of the challenge because, inter alia, "Adkinson consented to T-Mobile collecting and sharing his cell-site information. A defendant can voluntarily consent in advance to a search as a condition of receiving contracted services." *Adkinson*, 916 F.3d at 610.

a user's designated privacy preference, undercutting the assertion that the subjective expectation of privacy, the first step of the *Katz* two-part test, is "dead."[189]

A similar shift is evident in decisions that rely on service agreements in assessing privacy rights. Indeed, with such agreements, the tendency is even more pronounced as courts—applying contract principles to determine whether a user voluntarily waives a privacy right in their information—conclude that vague agreements undercut government claims of waiver.[190] The consequences of this shift are not only substantive; they are also procedural. By framing the question in terms of consent, which the government bears the burden of establishing,[191] the litigation dynamic shifts in favor of users.

In the next Part, we explore how courts might further operationalize contract tools of construction and interpretation when assessing Fourth Amendment privacy claims in the online environment.

III. TEXT, CONTEXT, AND THE REASONABLE EXPECTATION OF PRIVACY

As this Part explains, judicial use of contract tools to assess privacy expectations is not without historical precedent. In some cases, courts construe contracts to waive a privacy expectation, while in others they find a right preserved. The decisions, combined with the growing body of research findings concerning the experience of users with online service agreements and website applications and designs, illuminate the ways in which contract doctrine can be used in the assessment of Fourth Amendment online privacy claims.

189. Orin S. Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113, 114 (2015); *see also id.* at 133 ("[T]he subjective prong has become a phantom doctrine . . . . As a practical matter, the *Katz* test is only one step. The objective test is the only one that matters.").

190. *See* Warshak v. United States (*Warshak II*), 532 F.3d 521, 526–27 (6th Cir. 2008) (stating that "the expectation[] of privacy that computer users have in their e-mails . . . assuredly shifts from internet-service agreement to internet-service agreement," depending on the specific terms contained in ISP agreements).

191. Schneckloth v. Bustamonte, 412 U.S. 218 (1973) (noting that the state bears the burden of demonstrating that consent to a search is voluntary).

A. THE FOURTH AMENDMENT AND PRIVATE ORDERING

The online-related decisions discussed in Part II track the approach taken in other contexts. In these cases, contractual terms and relationships can define reasonable expectations of privacy, waiving them in some cases, and failing to waive them or even creating them in others.

1. Contracts Can Shape the Reasonable Expectation of Privacy

In *Zap v. United States,*[192] the Supreme Court allowed a quid pro quo waiver of privacy based on a contract provision. Zap, an engineer, entered into a contract with the federal government, and a term in the contract required that he submit to a search of his account and billing records.[193] A search of the records resulted in fraud charges brought against Zap.[194] The Court affirmed the validity of the search provision in the contract, finding a valid waiver based on a negotiation undertaken "in order to obtain the government's business."[195]

In *City of Ontario v. Quon*,[196] police officers were disciplined for sending sexually explicit texts on pagers provided by their employer. The agreement signed by the officers specified that their texts were subject to review, but supervisors promised at least one of the officers that so long as he paid for his text overages, his texts would not be audited.[197] The Ninth Circuit Court of Appeals held that the "operational reality" of these promises superseded the contractual language.[198] The Supreme Court reversed, looking to the employment agreement the officers signed, which notified them that the department would monitor texts.[199]

In *Dykes v. Southeastern Pennsylvania Transportation Authority*,[200] the Third Circuit Court of Appeals held that a public employer did not violate a former employee's Fourth Amendment rights when it required him to submit to suspicionless drug and alcohol testing, because his union's collective bargaining agreement prescribed the testing process. The process, to which

192. 328 U.S. 624 (1946).

193. *Id.* at 627.

194. *Id.*

195. *Id.* at 628.

196. 560 U.S. 746 (2010).

197. *Id.* at 752.

198. Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 907 (9th Cir. 2008), *rev'd*, *Quon*, 560 U.S. at 758.

199. *Quon*, 560 U.S. at 758.

200. 68 F.3d 1564, 1567–69 (3d Cir. 1995).

the employee agreed, effectively took precedence over a Fourth Amendment inquiry into individualized reasonable suspicion. The *Dykes* court noted that consent to an alternate process could be explicitly included in a collective bargaining agreement, or "implicit, derived from practice, usage and custom."[201]

Courts in employment cases exhibit a similar sensitivity to contractual language. They find that contracts between employees and employers can determine the reasonable expectation of privacy with regard to the actionability of privacy torts,[202] and the parameters of regulators' investigations.[203] As the Ninth Circuit Court of Appeals stated in one case: "It is clear that a contract may under appropriate circumstances diminish (if not extinguish) legitimate expectations of privacy,"[204] although this power is not unlimited.[205]

In other cases, a contractual right to a place or thing is sufficient to establish a privacy expectation. For example, in *United States v. Karo*,[206] the Supreme Court noted that "[a] person who rents out a hotel room or storage locker enjoys Fourth Amendment rights in the rented space so long as he complies with the rental contract."[207] Similarly, defendants have standing to challenge the stop of a taxicab because the contractual relationship

201. *Id.* at 1569. *See also*, *e.g.*, United States v. Angevine, 281 F.3d 1130, 1134 (10th Cir. 2002) ("University policies and procedures prevent its employees from reasonably expecting privacy in data downloaded from the Internet onto University computers."); Jinzo v. City of Albuquerque, 185 F.3d 874 (10th Cir. 1999) (rejecting employee's argument that the contract with the city was an unenforceable contract of adhesion, and holding that pursuant to the contract he had waived his Fourth Amendment rights).

202. *See, e.g.*, Jackson v. Liquid Carbonic Corp., 863 F.2d 111, 118–19 (1st Cir. 1988) (holding employee's invasion of privacy claim preempted by a collective bargaining agreement).

203. *See, e.g.*, Dir. of the Office of Thrift Supervision v. Ernst & Young, 795 F. Supp. 7, 10 (D.D.C. 1992) (finding that employees and partners of accounting firm had no reasonable expectation of privacy in work-related diaries kept in their offices for business reasons).

204. Yin v. State of Cal., 95 F.3d 864, 872 (9th Cir. 1996); *cf. In re* Von Der Ahe, 85 F. 959, 960 (W.D. Pa. 1898) (recognizing that the bounty hunter's arrest "is not made by virtue of the process of a court, but is the exercise of a right arising from the relation between the parties").

205. *See* United States v. Scott, 450 F.3d 863, 867–68 (9th Cir. 2006) ("While government may sometimes condition benefits on waiver of Fourth Amendment rights—for instance, when dealing with contractors [citing, *inter alia*, *Yin*]—its power to do so is not unlimited.").

206. 468 U.S. 705 (1984).

207. Orin S. Kerr, *The Fourth Amendment and New Technologies:*

allows the passenger to exclude others and control destination.[208]

2. Privacy Rights Preserved in the Absence of an Express Waiver

Byrd v. United States[209] affords a recent example of the way in which courts can read contracts narrowly to avoid waiver of an individual's privacy rights. In *Byrd*, the government unsuccessfully argued that the defendant had no reasonable expectation of privacy when the rental car he was driving (with the permission of the renter) was stopped by police, because he was not an approved driver according to the terms of the rental agreement.[210] On its face, the Court's decision seemingly rejected the role of contract in assessing whether an individual has a privacy expectation sufficient to provide standing, but closer analysis reveals that in fact construction of the contract drove the outcome. The six-member majority in *Byrd* emphasized that the contract itself did not undercut the defendant's reasonable expectation of privacy.[211] Although the contract expressly barred unauthorized drivers, such as Byrd, the only penalty for violation it provided was the voiding of insurance coverage; it did not pretermit any right to privacy in the vehicle.[212] Because the Court construed the contract narrowly, the defendant's expectation of privacy was not defeated.

Similarly, lower courts have held that students who consent to a university search of their premises are not held to consent to a police search.[213] It is also accepted that an apartment rental

Constitutional Myths and the Case for Caution, 102 MICH. L. REV. 801, 810–11 (2004) [hereinafter Kerr, *New Technologies*] (suggesting cases like *Karo* are grounded more in property than contract law).

208. *See, e.g.*, United States v. Woodrum, 202 F.3d 1, 6 (1st Cir. 2000); *cf.* O'Connor v. Ortega, 480 U.S. 709, 717–19 (1987) (holding in the context of the employment relationship that a doctor had a reasonable expectation of privacy in a desk and file cabinets used at work).

209. 138 S. Ct. 1518 (2018).

210. *Id.*

211. *See id.* at 1524 ("[A]s a general rule, someone in otherwise lawful possession and control of a rental car has a reasonable expectation of privacy in it even if the rental agreement does not list him or her as an authorized driver.").

212. *Id.* at 1528–29.

213. *See, e.g.*, Commonwealth v. Neilson, 666 N.E.2d 984, 987 (Mass. 1996) (holding a residence contract between student and university consenting to the university's search of the room did not give sufficient, express consent for the police to search the room); State v. Rodriguez, 521 S.W.3d 1, 20 (Tex. Crim. App.

agreement allowing a landlord to conduct unannounced inspections does not reduce the renter's reasonable expectation of privacy vis-à-vis the police.[214] Nor is the general consent provided to hotel staff to clean a room or repair appliances inside taken as a waiver of a renter-defendant's privacy rights in a room.[215]

B. CONSTRUING INTERNET STANDARD FORM AGREEMENTS IN CONTEXT

We now turn to the more specific context of the Internet. Privacy rights in the online environment are ostensibly based in significant part upon terms of service and privacy policies embodied in standard form contracts. For example, Facebook's boilerplate purports to govern all interactions with users,[216] and could affect whether they have waived rights against police searches.[217] Facebook's data policy likewise claims the privilege to "access, preserve and share your information with regulators, law enforcement or others . . . [i]n 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."[218] Understanding the proper construction of these terms requires knowledge of their formation, the content of their standard terms, and what

2017) ("[A] student does not assume the risk that university administrators will invite others—police officers—into the student's dorm room simply by living in a university dorm room pursuant to a contract allowing the university to make health safety inspections."). *But see* State v. Hunter, 831 P.2d 1033, 1035–37 (Utah Ct. App. 1992) (holding that university officials can search a dorm, even if accompanied by a police officer, at least where the officer is not directly involved in the search).

214. O'Connor v. Ortega, 408 U.S. 709, 730 (1987).

215. Stoner v. California, 376 U.S. 483, 489–90 (1964).

216. *Terms of Service*, FACEBOOK, https://www.facebook.com/terms.php [https://perma.cc/DD2D-SJ7J] (detailing Facebook's terms, which purport to "govern your use of Facebook . . . and the other products, features, apps, services, technologies, and software we offer").

217. Facebook's policy broadly provides that it will:

> access, preserve, and share your information with regulators, law enforcement, or other [officials] . . . [w]hen 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.

Data Policy, FACEBOOK, https://www.facebook.com/about/privacy/update [https://perma.cc/RP2A-UQZM].

218. *Id.*

contract doctrines teach us about their interpretation and enforceability. It also requires understanding the context in which consumers engage with service provider platforms.

1. The Enforceability of Boilerplate: Adhesion, Unconscionability, and Notice

The standard account of contract law imagines an arm's-length negotiation between co-equal, sophisticated parties. Research, however, has long shown that the account does not necessarily reflect market realities. This is because firms very often offer consumers boilerplate or standard form terms on a "take it or leave it" basis. Doing so has obvious major efficiency benefits for firms.[219] A seller with millions or billions of customers, such as Facebook, cannot reasonably negotiate with each one directly.[220] Standard forms can also financially benefit consumers, if sellers pass along transaction-related savings to consumers.[221]

Yet courts are often justifiably troubled by the use of agreements "to be signed by the party in [the] weaker position, usually a consumer, who adheres to the contract with little choice about the terms."[222] Contracts of this type are sometimes referred to as contracts of adhesion, and are subject to heightened judicial scrutiny because they are not negotiated in the classic sense.[223]

219. *See* ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1451 (7th Cir. 1996) (quoting RESTATEMENT (SECOND) OF CONTRACTS § 211 cmt. a (AM. LAW INST. 1981)) ("Standardization of agreements serves many of the same functions as standardization of goods and services; both are essential to a system of mass production and distribution. Scarce and costly time and skill can be devoted to a class of transactions rather than the details of individual transactions.").

220. *Id.*

221. *See, e.g.*, Robert A. Hillman, *Rolling Contracts*, 71 FORDHAM L. REV. 743, 747 (2002); Todd D. Rakoff, *Contracts of Adhesion: An Essay in Reconstruction*, 96 HARV. L. REV. 1174, 1230 (1983).

222. Quilloin v. Tenet HealthSystem Phila., Inc., 673 F.3d 221, 235 (3d Cir. 2012); *see also* K. N. Llewellyn, *The Standardization of Commercial Contracts in English and Continental Law by O. Prausnitz*, 52 HARV. L. REV. 700, 704 (1939) (arguing that contractual rights should not be governed by "the conditions and clauses . . . which happen to be printed on the unread paper, but [ ] those which a sane man might reasonably expect to find on that paper").

223. *See generally* Jay P. Kesan et al., *A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy*, 91 IND. L.J. 267, 285–86 (2016) (noting same and citing as examples, inter alia, *Bragg v. Linden Research, Inc.*, 487 F. Supp. 2d 593, 605 (E.D. Pa. 2007); *People v. Network Assocs., Inc.*, 758 N.Y.S.2d 466 (N.Y. Sup. Ct. 2003)).

When courts deem adhesive terms binding they do so at significant cost to consumers who very often lack the ability to self-protect.[224]

At times, contracts of adhesion are deemed unenforceable even in the face of evidence of ostensible consent, if the terms of the deal are procedurally or substantively unconscionable.[225] An agreement is procedurally unconscionable when unequal bargaining power leads to surprise or distress.[226] Courts question whether the party with weaker bargaining power truly consented to the deal.[227] An agreement is substantively unconscionable when it is clearly unfair, too one-sided, or otherwise against public policy.[228] An unconscionable privacy waiver might be construed against the drafter[229] or not enforced at all,[230] preserving the privacy rights of vulnerable parties.[231] Courts that refuse to

224. *See* Wayne R. Barnes, *Toward A Fairer Model of Consumer Assent to Standard Form Contracts: In Defense of Restatement Subsection 211(3)*, 82 WASH. L. REV. 227, 272–73 (2007).

225. *See, e.g.*, Dillard v. Merrill Lynch, Pierce, Fenner & Smith, Inc., 961 F.2d 1148, 1154 (5th Cir. 1992) (finding contracts of adhesion are not always void but rather are void only if they are also shown to be unconscionable); Armendariz v. Found. Health Psychcare Servs., Inc., 6 P.3d 669, 690 (Cal. 2000) (concluding that both procedural and substantive unconscionability must be present for a court to refuse to enforce a contract).

226. *See, e.g.*, Bischoff v. DirecTV, Inc., 180 F. Supp. 2d 1097, 1107 (C.D. Cal. 2002).

227. *Cf.* David T. Reindl, *Bargains or Unconstitutional Contracts? How Enforcement of Probation Orders as Contracts Could Take the Reasonableness out of Probation Searches*, 33 NEW ENG. J. ON CRIM. & CIV. CONFINEMENT 123, 145–51 (2007) (discussing ways in which significant disparate bargaining advantage by government in parole agreements renders the agreements themselves essentially contracts of adhesion).

228. Bank of Ind., Nat'l Ass'n v. Holyfield, 476 F. Supp. 104, 110 (S.D. Miss. 1979) (discussing unconscionability and finding the contract at issue too one-sided and therefore unconscionable). Contracts of adhesion are often found unenforceable only if they are also unconscionable. *See*, *e.g.*, Andrew A. Schwartz, *Consumer Contract Exchanges and the Problem of Adhesion*, 28 YALE J. ON REG. 313, 354–55 (2011).

229. *See, e.g.*, Daniel v. Ford Motor Co., 806 F.3d 1217, 1225 (9th Cir. 2015) ("The ambiguity, which is without question within a contract of adhesion, must be resolved against the draftsman."); *In re* RealNetworks, Inc., No. 00-C-1366, 2000 WL 631341, at *5 (N.D. Ill. May 8, 2000) ("[B]urying important terms in a 'maze of fine print' may contribute to a contract being found unconscionable . . . .").

230. RESTATEMENT (SECOND) OF CONTRACTS § 208 cmt. a (AM. LAW INST. 1981).

231. *See* William McGeveran, *Programmed Privacy Promises: P3P and Web Privacy Law*, 76 N.Y.U. L. REV. 1812, 1845 (2001) (arguing that contract law is

enforce contracts of adhesion on grounds of unconscionability attempt to correct for disparities in bargaining power that enable "oppression and unfair surprise."[232]

Adhesion warrants particular attention in light of the growing body of research underscoring the knowledge deficits and unequal bargaining position of consumers in the virtual space. Research shows that few people read user agreements regarding websites, social network platforms, or cellphone applications.[233] Moreover, they often fail to understand the typically lengthy and complex agreements even when read,[234] and do not understand how privacy settings function.[235] Some commentators suggest

more hospitable than property doctrine to privacy needs, pointing to "contract doctrines such as unconscionability [that] routinely protect vulnerable parties rather than leaving them at the market's mercy").

232. U.C.C. § 2-302 cmt. 1 (AM. LAW INST. & UNIF. LAW COMM'N 1977); JOSEPH M. PERILLO, CALAMARI & PERILLO ON CONTRACTS 388–89, 399 (5th ed. 2003) (noting cases disavowing the duty to read when adhesion or evidence of unconscionability is present, and recognizing that unconscionability might follow from transactions with unequal bargaining power or where oppression and unfair surprise could occur).

233. *See, e.g.*, James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1181–82 (2009) [hereinafter Grimmelmann, *Saving Facebook*] (citing a 2001 poll concluding that only three percent of survey participants claimed to carefully read privacy policies "most of the time," and a 2007 poll reporting that only thirty-one percent claimed to do so); Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 NW. U. L. REV. 139, 178 (2016) (discussing a study of cell phone users finding that ninety percent neither read the privacy policy offered by their provider nor even skimmed it in detail); Ari Ezra Waldman, *A Statistical Analysis of Privacy Policy Design*, 93 NOTRE DAME L. REV. ONLINE 159, 166 (2018) [hereinafter Waldman, *Privacy Policy Design*] (reporting study of 513 individuals finding that fewer than nine percent read privacy policies "always" or "often," and only approximately twelve percent correctly answered two questions about the legal implications of privacy policies).

234. *See, e.g.*, Imrul Kayes & Adriana Iamnitchi, *Privacy and Security in Online Social Networks: A Survey*, 3 ONLINE SOC. NETWORKS & MEDIA 1, 8 (2017) (citing and discussing studies); Jasmine McNealy, *The Privacy Implications of Digital Preservation: Social Media Archives and the Social Networks Theory of Privacy*, 3 ELON L. REV. 133, 142–44 (2012) (same). *See generally* Kevin Litman-Navarro, *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster*, N.Y. TIMES (June 12, 2019), https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html [https://perma.cc/USZ5-UB5R] (analyzing complexity of 150 privacy policies).

235. *See, e.g.*, Lauren Gelman, *Privacy, Free Speech, and "Blurry-Edged" Social Networks*, 50 B.C. L. REV. 1315, 1329 (2009) (citing study of college students showing that "between twenty and thirty percent did not know how Facebook's privacy controls worked, how to change them, or even whether they themselves had ever changed them").

that consumers use modern technology tools in blissful ignorance of privacy policies because ultimately they care little about their privacy.[236] However, considerable evidence suggests that consumers are actually interested in more privacy protective options than firms commonly provide,[237] and expect greater privacy rights than they are entitled to under a strict reading of user agreements.[238]

Despite users' (perhaps) rational ignorance,[239] classic contract doctrine would hold them bound by these privacy provisions.[240] Failure to read is generally not a defense against an

236. *See, e.g.*, Grimmelmann, *Saving Facebook*, *supra* note 233, at 1179 (summarizing the argument). In the privacy field, this is often referred to as the "privacy paradox": individuals express great concern about their online privacy but actually do little to protect it, for instance by submitting to the default privacy settings on Facebook. As researchers have pointed out, however, there are many explanations for the apparent disconnect, including the operation of cognitive biases, informational asymmetries regarding risk, and other obstacles such as the opacity of user agreements. *See generally* Spyros Kokolakis, *Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon*, 64 COMPUTERS & SECURITY 122 (2017) (summarizing the frequent inconsistency of privacy attitudes and behavior).

237. *See* Alireza Heravi et al., *Information Privacy in Online Social Networks: Uses and Gratification Perspective*, 84 COMPUTERS IN HUM. BEHAV. 441, 443 (2018) (citing studies). The point is highlighted by survey data comparing exposure of personal data to machines, as opposed to humans. *See* Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 628 (2011) (noting that while "the available evidence indicates that Internet users do not consider disclosure of their online information to automated equipment to be a privacy harm in and of itself," they nonetheless "consider disclosure of their information to other human beings to be a substantial harm" and have in fact been "actively hostile to the latter"); *see also* Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22 INFO. SYS RES. 254 (2011) ("When [privacy policy] information is [clearly and compactly displayed], consumers tend to purchase from online retailers who better protect their privacy.").

238. *See, e.g.*, Paul van Schaik et al., *Security and Privacy in Online Social Networking: Risk Perceptions and Precautionary Behaviour*, 78 COMPUTERS IN HUM. BEHAV. 283, 284–85 (2017) (discussing studies reflecting the disconnect). *See generally* Deirdre K. Mulligan & Jennifer King, *Bridging the Gap Between Privacy and Design*, 14 U. PA. J. CONST. L. 989, 1026 (2012) (describing how firms fail to correctly anticipate consumer desire for privacy and how FTC consent orders have required firms to better account for those desires).

239. *See* Richard A. Epstein, *Contract Not Regulation: UCITA and High-Tech Consumers Meet Their Consumer Protection Critics*, *in* CONSUMER PROTECTION IN THE AGE OF THE "INFORMATION ECONOMY" 227 (June K. Winn ed., 2006) (noting "rational ignorance" among consumers who eschew reading contracts in order "to economize on the use of our time").

240. *See, e.g.*, Darnaa, LLC v. Google, Inc., No. 15-CV-03221-RMW, 2015 WL

otherwise enforceable contract.[241] Like other contracting parties, consumers who engage with online firms are subject to a duty to read agreements.[242] Consumers, however, only have a duty to read contractual language when they have a reasonable opportunity to read it and when the language is understandable.[243] Therefore, questions of enforceability turn on whether consumers were sufficiently notified of contract terms when they first used the service[244] and whether they were notified of any changed terms thereafter.[245]

Shifting terms create challenges for consumers and courts alike. In the online context, courts have held that when a firm presents terms in a conspicuous manner, use of a "clickwrap" license that requires the consumer to click a box before continuing use satisfies notice, even though it is understood that no one reads those terms.[246] Courts have also held that an individual

7753406, at *2 (N.D. Cal. Dec. 2, 2015) (upholding use of the terms of service despite the fact that the plaintiff did not read the terms); Song Fi, Inc. v. Google Inc., 72 F. Supp. 3d 53, 62–63 (D.D.C. 2014) (upholding use of YouTube's terms of service despite the fact that "Plaintiffs lacked bargaining power"). *But see* PERILLO, *supra* note 232, at 388–89, 399.

241. *See, e.g.*, Allen v. Reynolds, 186 P.3d 663, 667 (Idaho 2008) (citations omitted) ("[A] party's failure to read a contract will not excuse his performance.").

242. *See, e.g.*, Feldman v. Google Inc., 513 F. Supp. 2d 229, 236–38 (E.D. Pa. 2007) (holding that the plaintiff had the duty to read terms that were presented in a scroll box and was required a click to agree).

243. *See* Heather Daiza, *Wrap Contracts: How They Can Work Better for Businesses and Consumers*, 54 CAL. W. L. REV. 201, 211–12 (2017) ("When consumer contracts are functionally unreadable . . . the duty to read becomes conceptually unfair.").

244. Specht v. Netscape Comm.'s Corp., 306 F.3d 17, 31–32 (2d Cir. 2002).

245. Douglas v. U.S. Dist. Ct. for Cent. Dist. of Cal., 495 F.3d 1062, 1062–63, 1066 (9th Cir. 2007).

246. *See, e.g.*, Nicosia v. Amazon.com, Inc., 834 F.3d 220, 238–39 (2d Cir. 2016) (recognizing in dicta that click-wrap agreements were an easy way to establish mutual consent, although Amazon did not use one).

can effectively consent to an unread contract by a change in conduct.[247] Moreover, when boilerplate changes, but consumer behavior does not change, consumers have been bound by new terms.[248]

Yet, it is also accepted that consumers are generally not held to consent to terms buried at the bottom of a web page, or on another linked page, unless their attention is clearly drawn to the link.[249] Indeed, the Federal Trade Commission has held that despite objective consent to standard form terms, failure to present terms clearly constituted an unfair and deceptive trade practice.[250] European regulators have likewise taken Facebook to task for fostering opportunities to disclose more information to more people, while burying options that allow consumers to restrict dissemination of information.[251]

In some cases, courts have shown sympathy for consumers subjected to changing terms. In *Douglas v. United States District Court*,[252] for instance, a cellphone provider, Talk America, added new terms of service, including an arbitration clause, to its website without directly notifying consumers. The district court concluded that the customer had accepted the new terms by paying his bill on line. The Ninth Circuit Court of Appeals disagreed, finding that Douglas "would have had no reason to look at the contract posted" online, and that he was under no

247. Galloway v. Santander Consumer USA, Inc., 819 F.3d 79, 87 (4th Cir. 2016) (concluding that plaintiff never "*explicitly* agreed to [defendant's] small modification to the Amended Agreement . . . [but] her making payment in the revised amount [defendant] requested and then continuing to make those payments for several years without complaint can only be interpreted as an assent to the terms of the Amended Agreement as slightly modified by the company").

248. *See, e.g.*, Boomer v. AT&T Corp., 309 F.3d 404, 424 (7th Cir. 2002) (noting that the customer did not cancel services after terms changed and thus was bound by the new terms); Hutcherson v. Sears Roebuck & Co., 793 N.E.2d 886, 887–88 (Ill. App. Ct. 2003) (holding that consumers consented to updated credit card terms by continuing to use the card); Jake Linford, *Unilateral Reordering in the Reel World*, 88 WASH. L. REV. 1395, 1407–08 (2013).

249. *Specht*, 306 F.3d at 35 ("We hold that a reasonably prudent offeree in plaintiffs' position would not have known or learned, prior to acting on the invitation to download, of the reference to [software] license terms hidden below the 'Download' button on the next screen.").

250. Complaint at 5, Sears Holdings Mgmt. Corp., F.T.C. Docket No. C-4264 (Aug. 31, 2009).

251. *Report of Audit: Facebook Ireland, Ltd.*, Office of the Data Protection Comm'r [Ireland] (2011).

252. 495 F.3d 1062, 1062–63, 1066 (9th Cir., 2007).

obligation to check for new terms.[253] Courts have also looked askance at agreements purporting to provide firms unfettered and unilateral ability to modify terms, deeming them illusory promises—promises that essentially promise nothing—which are unenforceable.[254]

To summarize, if consumers are on reasonable notice of the terms of a boilerplate contract,[255] and the firm proffering standard terms is making a promise that is not illusory,[256] the contract is generally enforceable. Courts might nevertheless find a contract unenforceable when it is unconscionable—because the deal, which comes in the form of a "take-it-or-leave-it" choice (as is standard with online service agreements),[257] is too one-sided or because consumers are unfairly surprised by the terms.[258]

An analogous situation arises when courts consider probation and parole agreements, where courts evince sensitivity to context and the power dynamic between the parties.[259] The Iowa Supreme Court's decision in *State v. Baldon* provides an instructive example.[260] In *Baldon*, the court concluded that an agreement signed by a parolee containing a prospective consent-to-search provision was insufficient, by itself, to establish the voluntary consent necessary to justify a suspicionless search under the Iowa Constitution.[261] In deeming the provision unenforceable, the court distinguished its prior precedent condoning consent provisions in probation agreements and the arms-length negotiated agreement addressed by the U.S. Supreme Court in *Zap*

253. *Id.* at 1066.

254. Grosvenor v. Qwest Corp., 854 F. Supp. 2d 1021, 1034 (D. Colo. 2012) ("[T]he unilateral power of one party to change the arbitration terms [ ] rendered the arbitration provisions illusory."); Harris v. Blockbuster Inc., 622 F. Supp. 2d 396, 399 (N.D. Tex. 2009).

255. *See supra* notes 240–53 and accompanying text.

256. *See supra* note 254 and accompanying text.

257. *See* Kayes & Iamnitchi, *supra* note 234, at 8–9 ("A second serious deterrent for users protecting their online privacy is the 'take-it-or-leave-it' 'choice' the users are offered. While it may seem like a free choice, in reality the cost of not using the online service . . . is unacceptably high.").

258. *See supra* text accompanying notes 222–32.

259. *See generally* Michael Chmelar, *Contract Law and its Potential Impact on Parole and Probation Searches*, 28 N. ILL. U. L. REV. 43, 54–56 (2007); Reindl, *supra* note 227.

260. 829 N.W.2d 785 (Iowa 2013).

261. *Id.* at 802–03. The provision provided that Baldon "would submit his 'person, property, place of residence, vehicle, [and] personal effects to search at any time . . . .'" *Id.* at 787.

(discussed above), reasoning that in those other contexts forfeiture of the Fourth Amendment right was the result of arms-length conscious bargaining.[262] "Generally," the court wrote, "courts enforce contracts because they are a product of the free will of the parties who, within limits, are permitted to define their own obligations."[263]

The consent term in the parole agreement, however, was not the result of arms-length bargaining, unlike a term in a probation agreement. Probationers "maintain a vastly superior bargaining power than parolees. Such a probationer has the choice of demanding a trial to seek his or her freedom, which many courts find gives rise to the type of bargaining power that renders probation agreements consensual."[264] The court concluded:

> Considering our obligation to ensure that consent remains a doctrine of voluntariness that functions with integrity, we conclude a parole agreement containing a prospective search provision is insufficient evidence to establish consent. Such a contract reveals an absence of bargaining power on behalf of the parolee, rendering contract principles inadequate to entitle the state to enforce compliance of a search provision. The purported consent extracted from a prisoner as a condition of release fails to constitute voluntary consent.[265]

Although online consumers face nothing like the coercive dynamic of an individual who must consent to a search term in order to be physically free of incarceration,[266] the relative impotence of the average consumer, faced with take it or leave it terms and conditions in standard boilerplate forms proffered by

262. *Id.* at 792–93.

263. *Id.*; *see also id.* at 801 ("The obligation of courts to examine the voluntariness of an agreement is nothing new and is supported by our law of contracts. For instance, we refuse to enforce unconscionable contracts . . . . The doctrine is especially applicable to contracts of adhesion."); *cf.* Colin Miller, *Plea Agreements as Constitutional Contracts*, 97 N.C. L. REV. 31 (2018) (surveying case law applying various contract law principles in assessing plea agreements).

264. *Baldon*, 829 N.W.2d at 795.

265. *Id.* at 802–03; *see also id.* at 802 ("[I]t is unreasonable to believe that the reality of consent normally derived from the benefits exchanged between the parties to a contract applies to parole agreements. The amount of freedom typically at stake points to the coercive nature of consent searches as a precondition to release.").

266. *See, e.g.*, Kari Paul, *Facebook, Google Privacy Settings Trick Consumers into Giving up Data, Consumer Groups Allege*, MARKETWATCH (June 29, 2018), https://www.marketwatch.com/story/facebook-google-privacy-settings-trick-consumers-into-giving-up-data-consumer-groups-allege-2018-06-28 [https://perma.cc/2WP9-MNT3] ("On Facebook, for example, when approving the company's privacy policies, users have the option to either 'accept' or 'delete account.'").

powerful firms, is striking.[267] The next section considers how courts should construe the boilerplate that purports to govern the on-line ecosystem.

2. Finding and Addressing Ambiguity in Online Boilerplate

Several basic precepts guide courts in determining the enforceability of boilerplate. Generally, "the intent of the parties at the time the contract is entered is controlling."[268] Under the orthodox view, optimal deals are those negotiated at arms-length and each party provides and receives valuable consideration.[269] When the contract is embodied in a writing, the "textual" or "formalist" approach directs courts to consider only the "four corners" of the agreement.[270] If the record suggests that the parties intended their agreement to be encompassed within the contractual terms, courts will not consider extrinsic or "parol" evidence as an aid in construing the contract.[271] Courts disagree about whether parol evidence is admissible to clarify written terms (so

267. *See* Julie E. Cohen, *Law for the Platform Economy*, 51 U.C. DAVIS L. REV. 133, 154–55 (2017).

268. Chuy v. Philadelphia Eagles Football Club, 595 F.2d 1265, 1271 (3d Cir. 1979). In assessing intent, courts adopt a primarily objective lens, considering the words and conduct of the parties rather than their subjective intentions. Joseph M. Perillo, *The Origins of the Objective Theory of Contract Formation and Interpretation*, 69 FORDHAM L. REV. 427, 427 (2000).

269. *See* R. Joseph Barton, *Drowning in a Sea of Contract: Application of the Economic Loss Rule to Fraud and Negligent Misrepresentation Claims*, 41 WM. & MARY L. REV. 1789, 1796 (2000) ("Contract law operates on the premise that contracting parties, in the course of bargaining for terms of a sale, are able to allocate risks and costs of the potential nonperformance. The underlying assumption is that the contract is the result of an arms-length negotiated transaction.").

270. *See, e.g.*, Steuart v. McChesney, 444 A.2d 659, 661 (Pa. 1982); Treemont, Inc. v. Hawley, 886 P.2d 589, 592–93 (Wyo. 1994).

271. *See, e.g.*, Telecom Int'l. Am. Ltd. v. AT&T Corp., 67 F. Supp. 2d 189, 202 (S.D.N.Y. 1999) (stating that, under New Jersey law, "[w]here a writing purports to be complete on its face, the writing must be accepted as the full expression of the agreement of the parties; parol evidence is not allowed"); *see also* Edith R. Warkentine, *Beyond Unconscionability: The Case for Using "Knowing Assent" as the Basis for Analyzing Unbargained-for Terms in Standard Form Contracts*, 31 SEATTLE U. L. REV. 469, 533–40 (2008) (summarizing the case law).

long as it does not vary or contradict them),[272] and whether it is admissible to establish ambiguity in the first instance.[273]

Courts seeking to resolve ambiguity in a contract will often construe ambiguous terms against the drafting party in close cases.[274] For instance, insurance company contracts are often construed against the drafting insurer.[275] Construing ambiguity against the drafter is sensible as a tie-breaking provision. One can reasonably presume that the drafter will take more care to protect his own interests than those of other contracting parties, and also more likely knows of and may be held responsible for existing ambiguities in contractual language.[276]

Such interpretive principles have particular resonance in the online context. A large body of research demonstrates that provisions in online standard form agreements and privacy policies are often ambiguous or unclear,[277] and can be intentionally

272. *Compare* McGraw-Hill Cos, Inc. v. Vanguard Index Trust, 139 F. Supp. 2d 544, 553 (S.D.N.Y. 2001) (holding that, under New York law, where meaning can be determined from contract language, a court is required to give effect to the contract as written and may not consider extrinsic evidence to alter or interpret its meaning), *with* Globus Medical, Inc. v. Vortex Spine, LLC, 213 F. Supp. 3d 719 (E.D. Pa. 2016) (stating that under Pennsylvania law, parol evidence is admissible to explain, clarify, or resolve ambiguity, irrespective of whether the ambiguity is patent, created by the language of the instrument, or latent, created by extrinsic or collateral circumstances).

273. *Compare* W.W.W. Assocs., Inc. v. Giancontieri, 566 N.E.2d 639, 642 (N.Y. 1990) (internal quotations omitted) ("It is well settled that extrinsic and parol evidence is not admissible to create an ambiguity in a written agreement which is complete and clear and unambiguous upon its face."), *with* Pacific Gas & Electric Co. v G. W. Thomas Drayage & Rigging Co., 442 P.2d 641, 644 (Cal. 1968) ("A rule that would limit the determination of the meaning of a written instrument to its four-corners merely because it seems to the court to be clear and unambiguous, would either deny the relevance of the intention of the parties or presuppose a degree of verbal precision and stability our language has not attained.").

274. RESTATEMENT (SECOND) CONTRACTS § 206 (AM. LAW INST. 1981) ("In choosing among the reasonable meanings of a promise or agreement or a term the[r]eof, that meaning is generally preferred which operates against the party who supplies the words or from whom a writing otherwise proceeds.").

275. *See, e.g.*, Ore & Chemical Corp. v. Eagle Star Ins. Co., Ltd., 489 F.2d 455, 457 (2d Cir. 1970). This rule is not so strong as to require courts to adopt an unreasonable interpretation. Intertherm, Inc. v. Coronet Imp. Corp., 558 S.W.2d 344 (Mo. Ct. App. 1977). Nor does the rule cut uniformly against knowledgeable parties, or those that had some role in the drafting process. Centennial Ent., Inc. v. Mansfield Dev. Co., 568 P.2d 50 (Colo. 1977).

276. RESTATEMENT (SECOND) CONTRACTS § 206, cmt. a (AM. LAW INST. 1981).

277. *See, e.g.*, Waldman, *Privacy Policy Design*, *supra* note 233, at 160 (citing

designed to make them inscrutable.[278] Indeed, privacy policies often are what Woodrow Hartzog calls "antiprivacy policies" that "provide a liability shield for companies looking to take advantage of users' failure to read."[279]

Courts over time have also adopted a less formalistic approach to assessing ambiguity, heeding context,[280] which has special significance in the online environment. For example, courts have used promissory estoppel to identify promises that the law should enforce. When a party makes a promise on which it would reasonably expect another party to rely, and the other party relies to their detriment, the promise is enforceable if injustice cannot otherwise be avoided.[281] Thus, as Hartzog has observed, if a firm makes a promise on its website on which users reasonably rely, it might be both reasonable and just to enforce the promise, whatever the standard form privacy policy might prescribe.[282]

Online firms can also make false promises in boilerplate, promising privacy with one provision and taking it away or limiting it with another, or by employing practices with the same effect. For example, in 2007, Facebook's privacy policy asserted both that users could "control the users with whom you share . . . information through [Facebook's] privacy settings," and that Facebook "share[s] your information with third parties only in limited circumstances."[283] Despite these assurances, Facebook

studies showing that "privacy policies are confusing, inconspicuous, long, and difficult to understand"); *see also* Joel R. Reidenberg et al., *Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding*, 30 BERKELEY TECH. L.J. 39, 40, 87–88 (2015) ("[A]mbiguous wording . . . undermines the ability of privacy policies to effectively convey notice of data practices to the general public.").

278. Waldman, *Privacy Policy Design*, *supra* note 233, at 160–61 (citing studies); Ari Ezra Waldman, *Privacy, Notice, and Design*, 21 STAN. TECH. L. REV. 74 (2018) (same).

279. WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 211 (2018).

280. RESTATEMENT (SECOND) CONTRACTS §§ 212–16 (AM. LAW INST. 1981); U.C.C. § 2-202 (AM. LAW INST. 2001).

281. Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1109 (9th Cir. 2009); RESTATEMENT (SECOND) CONTRACTS § 90 (AM. LAW INST. 1981).

282. *See* Woodrow Hartzog, *Promises and Privacy: Promissory Estoppel and Confidential Disclosure in Online Communities*, 82 TEMP. L. REV. 891 (2009) [hereinafter Hartzog, *Promises and Privacy*]; Woodrow Hartzog, *Website Design as Contract*, 60 AM. U. L. REV. 1635, 1661–62 (2011) [hereinafter Hartzog, *Website Design*].

283. *Facebook Principles*, (Sept. 12, 2007), https://web.archive.org/web/

launched its Beacon program, which extracted information from users' interactions with third-party websites and generated ads reflecting user activity, distributing the ads to users' friends without notifying users or asking their permission.[284] Facebook's behavior is not unique. A study by Robert Hillman and Ibrahim Barakat reported that many standard terms contained in "End User License Agreements" disclaim express warranties made on sellers' websites.[285]

Moreover, consenting to the use of information shared with Facebook or Google regarding targeted advertisements should not necessarily mean the user consents to Facebook or Google mining data for potential legal violations. Indeed, as Justice Gorsuch reminded us in his dissent in *Carpenter,* when an individual consents to some interactions and thus assumes some risk, this does not necessarily mean the individual consents to all interactions and assumes all associated risk.[286] Courts should reasonably understand that users might have consented to certain commercial exposure without necessarily waiving fundamental constitutional rights.

Thus, in construing the reasonable expectation of privacy in communications made on or through an ISP, a social networking platform, or a smartphone application, one cannot merely consider only boilerplate text. If courts seek to understand the deal consumers think they are getting, context is key.[287] In particular, as some courts have begun to recognize, whether disclosure

20070912083143/facebook.com/policy.php; *see also, e.g.*, *Is Dropbox Safe to Use?*, Dropbox, https://www.dropbox.com/help/security/safe-to-use [https://perma.cc/LQ6S-S8PK] ("Like most online services, we have a small number of employees who must be able to access user data for the reasons stated in our privacy policy (e.g., when legally required to do so).").

284. A class action settlement put an end to Beacon. *See* Lane v. Facebook, Inc., 696 F.3d 811 (9th Cir. 2012).

285. Robert A. Hillman & Ibrahim Barakat, *Warranties and Disclaimers in the Electronic Age*, 11 YALE J. L. & TECH. 1, 6 (2009).

286. *See* United States v. Carpenter, 138 S. Ct. 2206, 2263 (2018) (Gorsuch, J., dissenting); *cf.* PETER WESTEN, THE LOGIC OF CONSENT: THE DIVERSITY AND DECEPTIVENESS OF CONSENT AS A DEFENSE IN CRIMINAL CONDUCT 270–71 (2004) (citation omitted) (noting that a hockey player who implicitly consents to physical contact that is inherent and reasonably incidental to the game does not consent to an assault in excess thereof) [hereinafter WESTEN, THE LOGIC OF CONSENT].

287. *Cf.* Fernandez v. California, 571 U.S. 292, 303 (2014) (stating that whether a person consents to search should be based on "widely shared social expectations" and "customary social usage"); Florida v. Jardines, 569 U.S. 1, 9

waives Fourth Amendment rights should turn in significant part on how consumers interact with and utilize available privacy settings.[288] Firms provide them, but do not make them easy to locate or use[289] and often reset them without notice.[290] When consumers overcome these obstacles,[291] they signal their privacy preferences and expectations.[292] Consistent with the approach

(2013) (assessing authority of police to enter curtilage of a home by considering social norms expressed by "the scope of a license—express or implied").

288. *See, e.g.*, M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1030, 1033 (2013) (arguing that user experience can provide effective notice, warning or informing users about product features); Grimmelmann, *Saving Facebook*, *supra* note 233, at 1197 ("[W]hen users make privacy choices using Facebook's technical controls, they're expressing expectations about who will and won't see their information, and society should treat those expectations as reasonable for Fourth Amendment purposes."); Alireza Heravi et al., *Information Privacy in Online Social Networks: Uses and Gratification Perspective*, 84 COMPUTERS IN HUM. BEHAV. 441, 445 (2018) (discussing research regarding how this occurs); Alyson Leigh Young & Anabel Quan-Haase, *Privacy Protection Strategies on Facebook*, 16 INFO., COMM. & SOC. 479 (2013) (discussing variety of privacy-preserving strategies used by individuals on Facebook and the motivations behind them).

289. *See* Susanne Barth & Menno D.T. de Jong, *The Privacy Paradox—Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior—A Systematic Literature Review*, 34 TELEMATICS & INFORMATICS 1038, 1051 (2017) ("[S]uch [privacy] protection measures are not easily accessible while downloading and installing apps, suggesting that the majority of users do not possess the expertise nor the experience to engage in what would be considered appropriate protective behavior."); Brian Barrett, *The Facebook Privacy Setting that Doesn't Do Anything at All*, WIRED (Mar. 27, 2018), https://www.wired.com/story/facebook-privacy-setting-doesnt-do-anything/ [https:/perma.cc/LY9E-VJ5A] ("[F]ine-tuning what data friends, advertisers, and apps can access is a slog. The menus are labyrinthine, the wording obtuse."). Indeed, European regulators recently accused Facebook of "purposefully making it difficult for users to increase privacy protections on their sites." Paul, *supra* note 266.

290. *See, e.g.*, Matthew Keys, *A Brief History of Facebook's Ever-Changing Privacy Settings*, MEDIUM, (Mar. 21, 2018), https://medium.com/@matthewkeys/a-brief-history-of-facebooks-ever-changing-privacy-settings-8167dadd3bd0 [https://perma.cc/9QV4-YD6B] (documenting yearly, major shifts in Facebook's default settings from 2008–2018); *see also supra* text accompanying notes 246–54.

291. Nick Bilton, *Price of Facebook Privacy? Start Clicking*, N.Y. TIMES (May 12, 2010), https://www.nytimes.com/2010/05/13/technology/personaltech/13basics.html [https://perma.cc/A7UK-L3GP] (reporting that "[t]o opt out of full disclosure of most information, it is necessary to click through more than 50 privacy buttons, which then require choosing among a total of more than 170 options").

292. Philip Fei Wu, *The Privacy Paradox in the Context of Online Social*

taken by several courts,[293] such efforts warrant particular weight in assessing a user's reasonable expectation of privacy.[294]

The website designs navigated by users are also critically important. They too can delude users into thinking that they enjoy broader privacy protections than a firm actually provides.[295] A settlement between the Federal Trade Commission (FTC) and Snapchat illustrates how this can occur and why it is problematic.

The case concerned Snapchat, which started as a service that offered consumers the ability to send temporary, disappearing photo and video messages—"snaps"—through its cellphone application.[296] Eventually, the company became the target of an FTC investigation.[297] According to the FTC, Snapchat effectively promised in its marketing materials and through its user interface that users could "control how long . . . friends can view [a

Networking: A Self-Identity Perspective, J. ASS'N INFO. SCI. & TECH. 207, 213 (2019) (describing a positive relationship between user privacy management and perceived control over disclosure). According to Wu, "[p]rivacy settings in social information systems, therefore, are designed in such a way that a user's vulnerable 'true self' is shielded from external invasions." *Id.* at 208 (citing studies); *see also* Jessica Vitak et al., *Balancing Audience and Privacy Tensions on Social Network Sites*, 9 INTL J. COMM. 9 (2015) (discussing research on how the "imagined audience" of social media users affects privacy management); Wu, *supra*, at 210 (noting that users "rely on privacy management tools to define when to disclose what information with which 'imagined audience'").

293. *See supra* Part II.

294. *Cf.* Charles Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968) ("Privacy is not simply an absence of information about us in the minds of others; rather it is the *control* we have over information about ourselves."); *id.* at 483 (referring to one's ability to control information about oneself as "an aspect of personal liberty").

295. Here we build on the work of Woodrow Hartzog, who argued persuasively that "website features and design should, in some contexts, be considered enforceable promises." Hartzog, *Website Design*, *supra* note 282, at 1638. Hartzog proposes that courts use context to find that privacy preferences reasonably relied on create enforceable promises to preserve user confidentiality, or conclude that the manipulation baked into some website design makes the form contract unenforceable on unconscionability grounds. *Id.* at 1671. We expand on Hartzog's arguments by considering how the context of the platform experience should guide courts in determining whether users have waived Fourth Amendment rights to information shared on platforms.

296. Christine Elgersma, *Everything You Need to Know About Snapchat*, PHYS ORG (June 18, 2018), https://phys.org/news/2018-06-snapchat.html [https://perma.cc/8CU4-GWDA].

297. Erin Menshon, *FTC Cracks Down on Snapchat*, POLITICO (May 9, 2014, 9:00 AM), https://www.politico.com/story/2014/05/snapchat-ftc-privacy-crackdown-106495 [https://perma.cc/K9UP-VPGK].

sent] message."[298] Users could adjust, with a default maximum of ten seconds, the total time that the app would allow the recipient to view the snap before deletion. In various places, including FAQs and website architecture, Snapchat effectively promised users that photos would disappear forever, unless "quick" recipients took a screenshot of the image.[299] But Snapchat promised to warn consumers in those cases.[300] In reality, the snaps could often be stored indefinitely by recipients—and subsequently redistributed—without notice to users.[301]

Ultimately, the FTC determined that Snapchat's representations were false or misleading, and Snapchat submitted to a consent decree requiring, among other changes, that it no longer misrepresent the impermanence of snaps.[302] Thus, the FTC recognized in *Snapchat* that contextual signals, including adjustable settings, shaped the deal between the platform and its users, more particularly with regard to the promised scope of users' rights to privacy.[303]

Context that misrepresents the benefit the user receives from the website undermines the validity of consent, and calls into question whether the user voluntarily assumes the risk of further dissemination under the third party doctrine.[304] As Peter Westen argued vis-à-vis consent as a defense to criminal conduct, fraud "undermines" consent "not by causing [an individual] to believe that her position has thus changed for the worse, but by otherwise illicitly misleading her into believing that subjective [acquiescence to the interaction] is more beneficial than it really is."[305] Likewise, if a firm misrepresents through contex-

298. Complaint at 1, *In re* Snapchat Inc., No. C-4501, 2014 WL 7495798, F.T.C. Dec. 23, 2014).

299. *Snapchat Settles FTC Charges that Promises of Disappearing Messages Were False*, FED. TRADE COMM'N (May 8, 2014), https://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were [https://perma.cc/GTH9-SRER].

300. *See id*.

301. *Id.* at 2–3.

302. *Id.* at 7.

303. Complaint, *supra* note 298, at 4.

304. *See supra* Part I.

305. WESTEN, THE LOGIC OF CONSENT, *supra* note 286, at 188. Westen argues that fraudulent misrepresentations "preclude a person who relies upon them from being able to decide whether engaging in [an interaction with the misrepresenting actor] is truly in his or her interests." *Id.* at 189.

tual clues the benefits offered by using social networking services, that misrepresentation should vitiate consent to contrary boilerplate terms.

Therefore, to the extent a website's design represents that users can expect privacy and that privacy can be preserved by adjusting privacy settings, courts should give due weight to such representations when interpreting boilerplate. Consumers will reasonably see these contextual representations as part of the deal. These crucial contextual signals should affect the determination of privacy rights, especially when settings are inconsistent with boilerplate.

One might instinctively blanch at the notion that consumers can reasonably expect privacy in online contexts. As Woodrow Hartzog has noted, "the very function of online communities is to disseminate information."[306] This mindset drives decisions like *Everett*, where the court found no expectation of privacy because the defendant's Facebook settings allowed any "friend" to see posted information.[307]

Yet it is also true, as James Grimmelmann recognized, that firms like Facebook optimize their platform tools to promote the illusory perception that online conversations are akin to private conversations with close friends.[308] This slight-of-hand occurs in part because Facebook treats "friend" as a category capacious enough to include both intimate companions and casual or brand new acquaintances.[309] As Grimmelmann notes: "Facebook provides users with a forum in which they can craft social identities, forge reciprocal relationships, and accumulate social capital.

306. Hartzog, *Promises and Privacy*, *supra* note 282, at 919.

307. *See supra* notes 120–22 and accompanying text.

308. *See* Grimmelmann, *Saving Facebook*, *supra* note 233, at 1160 (noting that "Facebook systematically delivers signals suggesting an intimate, confidential, and safe setting").

309. *See* ARI EZRA WALDMAN, PRIVACY AS TRUST 97–99 (2018) [hereinafter WALDMAN, PRIVACY AS TRUST] (describing how privacy law often erroneously treats all disclosures no matter the relationship as a "public" disclosure that "erodes privacy rights"); Mulligan & King, *supra* note 238, at 1024 (arguing that the "proper question to ask [is] what sorts of information flows are necessary to support friendship. Such an inquiry [would] invite[] reflection on the differences between the vernacular category friend and the Facebook category Friend . . . ." It is worth noting that courts take a less than literal view of the Facebook "friend" designation in the judicial ethics context regarding judicial recusal. *See* Law Offices of Herssein & Herssein, P.A. v. U. S. Auto. Assoc., 271 So. 3d 889 (Fla. 2018).

These are important, even primal, human desires, whose immediacy can trigger systematic biases in the mechanisms that people use to evaluate privacy risks."[310] Firms capitalize on these desires by taking advantage of both the significant information asymmetries at work regarding privacy risks[311] and common inadequate (and yet over-confident) technological skills of users.[312] These companies also design their websites and apps to induce behavior that will increase user disclosures and thereby increase the volume of data shared through the platform,[313] which are subsequently mined and aggregated for profit.[314] As a result of this manipulative "'trust-based design,' users can be confused about the privacy effects of their behavior."[315] Additionally,

310. Grimmelmann, *Saving Facebook*, *supra* note 233, at 1151.

311. *See, e.g.*, Mark J. Keith et al., *Information Disclosure on Mobile Devices: Re-examining Privacy Calculus with Actual User Behavior*, 71 INT'L J. HUM. COMP. STUD. 1163 (2013) (examining information deficits regarding privacy risks among mobile device users and their negative effect on rational decision-making). *See generally* Han Li et al., *Understanding Situational Online Information Disclosure as a Privacy Calculus*, 51 J. COMPUT. INFO. SYS. 62 (2010) (discussing risk-benefit calculation that commonly drives individual decisions to disclose personal information and the negative impact of informational deficits).

312. *See, e.g.*, Moritz Büchi et al., *Caring Is Not Enough: The Importance of Internet Skills for Online Privacy Protection*, 20 INFO., COMM. & SOC'Y. 1261 (2017) (noting that individuals very often overestimate their skill with privacy-enhancing technologies); Carlos Jensen et al., *Privacy Practices of Internet Users: Self-reports Versus Observed Behavior*, 63 INT'L J. HUM. COMPUT. STUD. 203 (2005).

313. *See* Ari Ezra Waldman, *Privacy, Sharing, and Trust: The Facebook Study*, 67 CASE W. RES. L. REV. 193, 223 (2016) [hereinafter Waldman, *Privacy, Sharing, and Trust*] ("Facebook designs its platform and interface to leverage the trust we have in our friends to nudge us to share . . . . [Thus,] no Facebook design change can be understood independent of the platform's insatiable appetite for user data."). Facebook, moreover, is known to merge its data with that gathered from millions of third party websites and apps (some of which it owns) without users' consent, a practice recently prompting concern from European regulators. Bill Chappell, *Facebook Can't Gather Users' Data from Other Websites, German Antitrust Office Says*, NPR (Feb. 7, 2019), https://www.npr.org/2019/02/07/692312687/facebook-cant-gather-users-data-from-other-websites-german-antitrust-office-says [https://perma.cc/T5PL-GRBH].

314. Facebook appears quite aware of the consequences of its efforts, as revealed in a patent filing. Laura R. Ford, *Patenting the Social: Alice, Abstraction, & Functionalism in Software Patent Claims*, 14 CARDOZO PUB. L. POL'Y & ETHICS J. 259, 266 (2016) (emphasis in original) (noting that Facebook is "claiming to own methods, apparatuses, and computer systems that facilitate and manipulate people's *understandings and conceptions* of their social relationships").

315. Waldman, *Privacy, Sharing, and Trust*, *supra* note 313, at 193; *see also*

frequent changes in agreement terms can contribute to a fatigue effect[316] that aggravates the cognitive biases and deficits discussed.[317]

Moreover, some websites are designed to manipulate individuals into disclosing information they might otherwise prefer not to disclose.[318] For example, Facebook targets teenage users with advertisements when its algorithms predict they are likely to feel "worthless" and "insecure," allowing advertisers to serve up more effective ad content in moments of vulnerability.[319]

HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 225 (2010) (positing that in cases where users experience a "nasty surprise" about how a platform has used data, "we would find that [users] have understood themselves to be operating in one context and governed by the norms of that context, only to find that others have taken them to be operating in a different one"); WALDMAN, PRIVACY AS TRUST, *supra* note 309, at 56–60 (describing how trust shapes user willingness to share on platforms like Facebook); Paul, *supra* note 266 (quoting Finn Myrstad, Director of Digital Policy and Energy at the Consumer Council of Norway) ("Facebook and Google make us share personal information with cunning design, confusing interfaces, and take it or leave it options.").

316. Lindsey Barrett, *Model(ing) Privacy: Empirical Approaches to Privacy Law & Governance*, 35 SANTA CLARA HIGH TECH. L.J. 1, 42–46 (2018).

317. Although courts do not always invalidate change of terms clauses, the FTC has found that a retroactive privacy policy change is an unfair practice in at least two cases, one involving Facebook. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 640–41 (2014) (citing *In re* Gateway Learning Corp., 138 F.T.C. 443, 446, 449 (2004); Complaint at 9, *In re* Facebook, Inc., FTC File No. 0923184 (No. C-4365)). In the Facebook case, the FTC stated:

> [B]y designating certain user profile information publicly available that previously had been subject to privacy settings, Facebook materially changed its promises that users could keep such information private. Facebook retroactively applied these changes to personal information that it had previously collected from users, without their informed consent.

Id. at 641 n.287 (quoting Complaint at 9, F.T.C. File No. 0923184).

318. Hartzog, *Website Design*, *supra* note 282, at 1664 (citing GREGORY CONTI & EDWARD SOBIESK, MALICIOUS INTERFACE DESIGN: EXPLOITING THE USER (2010), http://www.rumint.org/gregconti/publications/201004_malchi.pdf); *see also* WOODROW HARTZOG, PRIVACY'S BLUEPRINT 208 (2018) (describing how website design often leads to inauthentic consent through the use of "[c]onfusing wording, nested menus, and other tricks to confuse and obfuscate consent mechanisms"); Han Li et al., *The Role of Affect and Cognition on Online Consumers' Decision to Disclose Personal Information to Unfamiliar Online Vendors*, 51 DECISION SUPPORT SYS. 434, 434 (2011) (reporting that consumers' privacy risk assessment changes as they interact with the website).

319. Sam Machkovech, *Report: Facebook Helped Advertisers Target Teens Who Feel "Worthless,"* ARS TECHNICA (May 1, 2017), https://arstechnica.com/

Thus, users of platforms like Facebook, YouTube, Google, or Twitter likely do not understand, or at least likely underestimate, how much data collectors and aggregators have acquired, and how that information allows those firms to "subvert our decision-making."[320]

It is thus not surprising that individuals like the student in *Chaney* (noted earlier) leave in place defaults that lead to the broadest possible access to information posted online.[321] In this environment, courts should view with skepticism changes in platform terms, especially when a change might undermine user rights to privacy, and avoid indulging in blithe assumptions that accepting a friend request equates with a privacy waiver.[322]

C. CONSTRUING CONTRACT TEXT IN CONTEXT

Given the problems with notice, consent, and manipulation discussed above, courts should generally construe ambiguity in terms of service against the drafter and in favor of the user. Thus, where there is ambiguity regarding a potential waiver of a privacy right, in some shape or form, the ambiguity should cut against waiver and in favor of preserving users' privacy rights.

Courts should endeavor to read text and context together.[323] If boilerplate, website design, and settings agree, courts have a substantial basis for determining whether privacy is waived. Conversely, standard form language might cut in one direction while contextual factors cut in the opposite direction. In such instances, promises made or promises disclaimed might be at odds with the lived reality of users as they engage with online service providers. Courts will then face a more difficult decision. We suggest the following resolutions.

information-technology/2017/05/facebook-helped-advertisers-target-teens-who-feel-worthless/ [https://perma.cc/6WYG-L9BK].

320. Daniel Susser et al., *Online Manipulation: Hidden Influences in a Digital World*, GEO. LAW TECH. R. (forthcoming) (manuscript at 2) (Dec. 23, 2018), https://ssrn.com/abstract=3306006 [https://perma.cc/S6NV-AEJV]; *see also* Karen Yeung, *Hypernudge: Big Data as a Mode of Regulation by Design*, 20 INFO., COMM. & SOC'Y (2016).

321. *See supra* notes 132–33 and accompanying text.

322. Ford, *supra* note 314, at 266.

323. *See generally* NISSENBAUM, *supra* note 315 (advancing a theory of "contextual integrity" in which contextual norms shape privacy protections); Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 DAEDALUS 32 (2011).

If, for example, the platform's design suggests that the firm respects privacy rights, but the boilerplate seems to allow for disclosure to third parties and the government, context should weigh heavily in favor of preserving users' rights.[324] This is particularly true for a user that has endeavored to restrict access to a narrower, more granular subset of individuals by adjusting offered privacy settings, difficult though that may be.[325] This is the more realistic, non-zero sum approach to online privacy recognized in cases like *Meregildo*, *DiTomasso*, *Ehling* and *Facebook v. Superior Court*.[326]

On the other hand, one could imagine the rare case when boilerplate text offers or creates privacy protections, but users behave in ways that suggest an intent to broadly disclose information. Both are relevant evidence about the disclosures to which the user consents. However, privacy settings are usually more salient.[327] Users can perceive, at least to some extent, the effect of settings as they interact with the platform and see how other users' profiles are presented. *Ceteris paribus*, users are less likely to rely on boilerplate language, and more likely to rely on settings and default disclosures, to the extent they are disclosed in an understandable manner.[328]

Finally, courts should not necessarily construe a decision to leave default settings in place in favor of waiver. As noted, the cognitive and behavioral pressures of platforms usually militate strongly in favor of easy data mining and broad disclosure. Given the hydraulic pressure applied by many platforms, courts should hesitate before presuming broad disseminations were intended as such, that every addition of a new "friend" was voluntary in a

324. *See* NISSENBAUM, *supra* note 315.

325. *See supra* notes 287–94 and accompanying text.

326. *See supra* Parts II.A–B; *see also* Lewis v. LeGrow, 670 N.W.2d 675 (Mich. App. 2003) (recognizing that privacy waiver is not a zero-sum question but rather turns on particular circumstances); Sherry F. Colb, *What Is a Sefarch? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 122 (2002) ("[T]reating exposure to a limited audience as identical to exposure to the world[] means failing to recognize degrees of privacy in the Fourth Amendment context."); Lucas Issacharoff & Kyle Wirshba, *Restoring Reason to the Third Party Doctrine*, 100 MINN. L. REV. 985, 985–86 (2016) (noting that the "third party doctrine turned heavily on the limited forms of interaction in a prior technological era. As society has changed, the presumption of limited means of dissemination has all but collapsed, and the scope of what is covered by the third party doctrine has thus expanded").

327. *See generally, e.g.*, Waldman, *Privacy Policy Design*, *supra* note 233.

328. *See* Calo, *supra* note 288, at 1033.

privacy-waiving sense, or that the platform's current distribution defaults are those to which a user initially agreed.[329]

More concretely, our analysis suggests different outcomes in certain cases. In cases where the government directly seeks to compel a platform or ISP to disclose user information, the attempt should be supported by a warrant, as in *Warshak* III.[330] Warrantless searches should be prohibited unless the terms of use make reasonably clear that the firm will actively assist law enforcement, as in *DiTomasso*; those terms are clearly presented and understandable; and users have not utilized a platform's privacy settings to limit the potential audience for communications, or otherwise been led to assume by the firm that their privacy would be protected.[331]

Such an approach aligns with the Supreme Court's recent conception of the third party doctrine in *Carpenter,* which held that the mere sharing of information with a third party does not eliminate a Fourth Amendment privacy interest.[332] Indeed, even more than the geo-locational information at issue in *Carpenter*,

329. One might also wonder whether decisions made by users when they signed on to a platform should bind them later? As James Grimmelmann has noted, people are generally time-inconsistent, becoming more concerned with privacy as they age. Younger people might not recognize the scope of potential disclosure, finding out only later how much they have lost—a costly way to develop an accurate view of disclosure defaults. Grimmelmann, *Saving Facebook*, *supra* note 233, at 1189.

330. *See supra* notes 179–81 and accompanying text.

331. This is essentially the position adopted by the American Bar Association in its recently approved standards concerning law enforcement access to third party records. *See* STANDARDS FOR CRIMINAL JUSTICE, LAW, ENFORCEMENT ACCESS TO THIRD PARTY RECORDS § 25-5.1(b) cmt. at 97 (AM. BAR ASS'N 2013), https://www.americanbar.org/groups/criminal_justice/standards/law_enforcement_access/ [https://perma.cc/U5XC-6Z5H] (requiring individualized consent, which "mean[s] that the agreeing party knew he or she could refuse permission and still take advantage of the desired service from this provider, and he or she specifically acknowledged [the] possibility of law enforcement access").

332. United States v. Carpenter, 138 S. Ct. 2206, 2221 (2018); *see also* City of Ontario v. Quon, 560 U.S. 746, 760 (2010) (recognizing that "[c]ell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification"); *cf.* Berger v. New York, 388 U.S. 41, 63–64 (1967) (recognizing protectable privacy interest in content of telephone conversations); *Ex Parte* Jackson, 96 U.S. 727, 733 (1878) (concluding that the content of mailed letters and sealed packages are "fully guarded from examination and inspection, except as to their outward form and weight").

online users' data (e.g., photos and writings) are "identifying information,"[333] certainly compared to the information disclosed in *Miller* and *Smith*.[334] Also, as in *Carpenter*, serious questions exist whether users "voluntarily" expose their information. Having an online presence, like carrying a cellphone, has become in the Court's words virtually "indispensable to participation in modern society,"[335] and online interactions figure centrally in social and political life.[336] Broad, unwarranted access of law enforcement to data gathered through those platforms may deleteriously degrade relationships and chill communication.[337]

A less compelling situation involves betrayal by a friend, who provides information to law enforcement.[338] Assuming arguendo that misplaced trust cases like *Hoffa*[339] were correctly decided, such betrayal is beyond the scope of Fourth Amendment protection.

333. *Carpenter*, 138 S. Ct. at 2212, 2219.

334. *See supra* notes 53–61 and accompanying text.

335. *Carpenter*, 138 S. Ct. at 2220 (citations omitted); *cf.* Katz v. United States, 389 U.S. 347, 352 (1967) (finding privacy right in telephone conversation because not doing so would "ignore the vital role that the public telephone has come to play in private communication"); People v. Sporleder, 666 P.2d 135, 141 (Colo. 1983) ("A telephone is a necessary component of modern life. It is a personal and business necessity indispensable to one's ability to effectively communicate in today's complex society.").

336. *See generally* Yongick Jeong & Erin Coyle, *What Are You Worrying About on Facebook and Twitter? An Empirical Investigation of Young Social Network Site Users' Privacy Perceptions and Behaviors*, 14 J. INTERACTIVE ADVERT. 51, 52 (2014) (summarizing research showing critical role played by Internet in social and political life).

337. Matthew Tokson, *The Normative Fourth Amendment*, 104 MINN. L. REV. (forthcoming 2019) (manuscript at 11) (arguing that Fourth Amendment law would be more normatively sound and capable of consistent application if courts explicitly weighed the value of surveillance practices against "three fundamental harms: the avoidance of lawful activity because of fear of surveillance; the harm to relationships and communications caused by observation; and the concrete psychological or physical harm suffered due to surveillance"); *see also* Jeong & Coyle, *supra* note 336, at 53 ("[W]hen a loss of control is perceived, related harmful consequences undermine a person's independence and increase a sense of vulnerability for the individual."); Tokson, *supra*, (manuscript at 24) (citing "numerous studies in which respondents rate the perceived invasiveness of various surveillance practices including location tracking, social media monitoring, and internet data collection").

338. Indeed, terms of use sometimes warn users of the dangers of false friends, as Omegle's terms warned DiTomasso. *See supra* notes 170–71 and accompanying text.

339. *See* Hoffa v. United States, 385 U.S. 293 (1966).

Before Facebook in particular redefined the concept of friend, one can imagine that individuals protected themselves from false friends, and endeavored to protect conversations as private, using social norms and trust mechanisms.[340] With some Facebook friends, users still have social leverage, and put sensitive information at the mercy of those friends with open eyes. As discussed above, however, Facebook manipulates user preferences, nudging, cajoling, and sometimes resetting defaults to increase friending and the amount and nature of information disclosed to those friends.[341]

What of instances involving police acting as "false friends," whereby a government agent gains entre into a user's online environ by a seemingly benign but false overture of friendship? Deception and trickery are time-honored, if controversial, tools of the law enforcement trade.[342] The ramifications of such strategies, in terms of corroding faith in one's fellow citizens, problematic enough in the face-to-face social world, are considerably more so in the online world, especially given what we know of the manipulative strategies and pressures exerted by firms.[343]

As one commentator observed in the pre-Internet era, in arguing for the need to reevaluate the police subterfuge cases post-*Katz*, "[t]o live with the knowledge that one's neighbor may eavesdrop is an experience different in kind and quality than to live with the knowledge that one's government secretly inserts its agents into one's personal and political affairs."[344] The difference was recognized by Justice Douglas in a largely forgotten, pre-*Katz* decision.[345] As Morgan Cloud recently summarized Justice Douglas's assessment of the distinction between misplaced trust in a friend and fakery by an officer:

> One could always legitimately disclose information to private citizens. If they later choose to take this information to the police, no constitutional issues would arise. But the architects of the Constitution erected

340. Ari Ezra Waldman, *Manipulating Trust on Facebook*, 29 LOY. CONSUMER L. REV. 175, 186–87 (2016) (describing the standard use of social norms to ensure trust).

341. *See supra* notes 308–16 and accompanying text.

342. *See generally* Elizabeth N. Jones, *The Good and (Breaking) Bad of Deceptive Police Practices*, 45 N.M. L. REV. 523 (2015).

343. *See supra* Part III.B.

344. Dolores A. Donovan, *Informers Revisited: Government Surveillance of Domestic Political Organizations and the Fourth and First Amendments*, 33 BUFF. L. REV. 333, 338 (1984).

345. Osborn v. United States, 385 U.S. 323, 341–43 (1966) (Douglas, J., dissenting).

> constitutional privileges like the Fourth Amendment precisely to limit government power. Disclosures to government agents are, in fact, different from those made to private citizens.[346]

If courts are persuaded that users surrender privacy as a result of what Professor Cloud terms their "ignorant consent" in the face of police subterfuge concerning identity, they will allow the misplaced trust doctrine to swamp every user's reasonable expectation of privacy,[347] in a context that has assumed critical importance in the marketplace of ideas and associations.[348] The Supreme Court's insistence that citizen knowledge only be a factor in assessing the voluntariness of consent to search,[349] which research shows is problematic in everyday street patrol,[350] is even more so in the online context, as the *ABA Standards* regarding police access to third party records suggest.[351]

One could imagine a less robust version of these proposals, inviting courts to discount the privacy-waiving effects of boilerplate text, or decisions not to adjust privacy settings, only if the user can establish that the platform in question attempted to de-

346. Morgan Cloud, *Ignorance and Democracy*, 39 TEX. TECH L. REV. 1143, 1168 (2007). Justice Harlan, dissenting in *United States v. White*, eloquently and at length urged reconsideration of the Court's condonation of surreptitious electronic monitoring by police because of the negative effect on society. 401 U.S. 745, 768 (1971). For an incisive treatment of Harlan's *White* dissent see Catherine Hancock, *Warrants for Wearing a Wire: Fourth Amendment Privacy and Justice Harlan's Dissent in* United States v. White, 79 MISS. L.J. 35, 45 (2009).

347. Neil Richards, *The Third-Party Doctrine and the Future of the Cloud*, 94 WASH. U. L. REV. 1441, 1482 (2017) ("[I]n a digital world, the simple intuition of misplaced trust applied universally threatens the end of the Fourth Amendment as we know it.").

348. *See supra* notes 5, 73–75, and accompanying text.

349. *See* Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973).

350. *See, e.g.*, Alafair S. Burke, *Consent Searches and Fourth Amendment Reasonableness*, 67 FLA. L. REV. 509 (2016); Janice Nadler, *No Need to Shout: Bus Sweeps and the Psychology of Coercion*, 2002 SUP. CT. REV. 153 (2002); James C. McGlinchy, Note, *"Was That a Yes or a No?" Reviewing Voluntariness in Consent Searches*, 104 VA. L. REV. 301 (2018).

351. *See* STANDARDS FOR CRIMINAL JUSTICE, LAW, ENFORCEMENT ACCESS TO THIRD PARTY RECORDS § 25-5.1(b) cmt. at 97 (AM. BAR ASS'N 2013), https://www.americanbar.org/groups/criminal_justice/standards/law_enforcement_access/ [https://perma.cc/U5XC-6Z5H] (requiring proof that "the focus of the record [request] has knowingly and voluntarily consented to that specific law enforcement access"); *see also id*. cmt. at 95 ("Only knowing and voluntary agreement constitutes consent. The Supreme Court has modified this traditional requirement for purposes of the Fourth Amendment, but for reasons that are rarely applicable to records acquisition.").

ceive in its settings or standard forms. Such an approach, however, would likely under-protect privacy rights, for at least two reasons. First, consumers are unlikely to have access to such evidence. Second, courts may perceive evidence of actual manipulation as too subtle to amount to outright deception, even though the literature reviewed above suggests that these platforms encourage user disclosure by engendering trust, in a context quite different from cases like *Smith* and *Miller*. Contextual assurances of privacy might be misconstrued, even though those assurances might not rise to the level of outright fraud.[352]

The foregoing guideposts will certainly limit the capacity of law enforcement to freely access users' online information. Rights, however, are not enshrined in the name of governmental efficiency.[353] The next Part considers how our approach might help courts establish a proper constitutional baseline for Fourth Amendment privacy rights in the online environment.

IV. IMPLICATIONS AND POTENTIAL CONCERNS

For reasons discussed, the model advocated here, drawing upon contracts doctrine to inform Fourth Amendment privacy analysis, is preferable to the justly condemned indeterminacy of the *Katz*-based expectation of privacy test. Its benefits, moreover, come into sharper focus when compared to arguments advanced in favor of several emerging competing models.

352. Calo, *supra* note 288, at 1065–66 (arguing that both false reassurances and deliberate deception can harm consumers). Consumers appear vulnerable to discounting fraudulent practices when they are backed up by boilerplate. *See* Meirav Furth-Matzkin & Roseanna Sommers, *Consumer Psychology and the Problem of Fine Print Fraud*, 72 STAN. L. REV. (forthcoming 2020) (reporting experimental studies in which laypeople presented with cases of fraud tend to believe that boilerplate is enforceable even when consent to a contract is fraudulently induced).

353. *See* Riley v. California, 573 U.S. 373, 403 (2014) ("The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant."); United States v. White, 401 U.S. 745, 756 (1971) (Douglas, J., dissenting) ("[T]he concepts of privacy which the Founders enshrined in the Fourth Amendment vanish completely when we slavishly allow an all-powerful government, proclaiming law and order, efficiency, and other benign purposes, to penetrate all the walls and doors which men need to shield them from the pressures of a turbulent life around them and give them the health and strength to carry on.").

One is an approach predicated on positive law.[354] Justice Gorsuch lauded its benefits in *Carpenter*,[355] asserting that "positive law may help provide detailed guidance on evolving technologies without resort to judicial intuition. State (or sometimes federal) law often creates rights in both tangible and intangible things."[356] His reasoning relied heavily on work by Will Baude and James Stern, who in a recent article argued that positive law should set the limits on the government's right to search. Baude and Stern assert that if a private individual can engage in a behavior leading to the discovery of information, the government should also be allowed to do it, and vice versa.[357] "If people want to live in fishbowls," Baude and Stern maintain, "the Fourth Amendment should not be what stops them, so long as the government swims alongside them."[358]

Although not without appeal, the positive law model is problematic for several reasons. As an initial matter, there can be a basic mismatch between the purpose of a law and the question whether privacy was (or was not) invaded. For instance, a law designed to promote safety, such as regulating the minimum altitude for air flights, does not speak to whether a search of a home (or its curtilage) occurred, even though the Court concluded otherwise in a pair of cases.[359] Moreover, as Richard Re argued in response to Baude and Stern's article, use of the positive law model could "create an incentive for lawmakers to adjust privacy protections for private parties so as to expand the power of law enforcement."[360] Perhaps most significantly, it is troublesome to think that simply because a private actor (including an

354. *Positive Law*, BLACK'S LAW DICTIONARY pg. 1182 (7th ed. 1999) (defining positive law as "[a] system of law promulgated and implemented within a particular political community by political superiors, as distinct from moral law or law existing in an ideal community or in some nonpolitical community. Positive law typically consists of enacted law—the codes, statutes, and regulations that are applied and enforced in the courts.").

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

356. *Id.* at 2270 (Gorsuch, J., dissenting).

357. William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1825–26 (2016).

358. *Id.* at 1866.

359. Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503,510, 533 (citing California v. Ciraolo, 476 U.S. 207 (1986); Florida v. Riley, 488 U.S. 445 (1989)).

360. Richard M. Re, *The Positive Law Floor*, 129 HARV. L. REV. F. 313, 321 (2016); *see also id.* at 329 (asserting that "when democratic pathologies arise, the positive law model would have perverse effects, causing defects in regular

ISP) is permitted to invade privacy, consistent with positive law, that law enforcement should also be able to do so.[361]

Another option, urged by Justice Alito in particular,[362] is to let legislatures devise laws that set privacy expectations and limit the authority of police to access information.[363] California, for instance, has an expansive Privacy Act that covers a vast range of communications and imposes significant limits on police authority to access information.[364]

Other states enacted laws regulating the use of geo-location data prior to the Court's decision in *Carpenter*,[365] as well as laws governing access to and use of Event Data Recorders ("black boxes") in cars.[366] Perhaps most famously, Congress, in the wake

lawmaking to curb the Fourth Amendment"); *id.* at 324 ("Because laws that formally apply to both private parties and the police often have the practical effect of favoring the police, automatic reliance on those laws would systematically underprotect Fourth Amendment values . . . .").

361. *See id.* at 314 ("[G]overnment action is different—and often more deserving of regulation—than similar conduct by private parties. Due to its distinctive capabilities, incentives, and social role, the government often threatens the people's security in ways that private parties simply do not."); *see also* Fernandez v. California, 571 U.S. 292, 313 (2014) (Ginsburg, J., dissenting) ("Police, after all, have power no private person enjoys. They can, as this case illustrates, put a tenant in handcuffs and remove him from the premises."). Moreover, Baude and Stern's positive law model only addresses the question of whether a "search" occurs, not the more vexing question of whether police behavior challenged is reasonable. Re, *supra* note 360, at 317–18.

362. *See, e.g.*, Riley v. California, 573 U.S. 373, 407–08 (2014) (Alito, J., concurring); United States v. Jones, 565 U.S. 400, 429–30 (2012) (Alito, J., concurring).

363. *See generally* Kerr, *New Technologies*, *supra* note 207, at 855 (surveying advantages of legislative approach).

364. *See* Susan Freiwald, *At the Privacy Vanguard: California's Electronic Communications Privacy Act (CalECPA)*, 33 BERKELEY TECH. L.J. 131 (2018).

365. *See, e.g.*, CONN. GEN. STAT. § 54-47aa (2017); 2014 MD. CODE ANN., CRIM. PROC. § 1-203.1 (West 2014); MINN. STAT. § 626A.42 (2014); N.H. REV. STAT. ANN. § 644-A (2015).

366. *Privacy of Data from Event Data Recorders: State Statutes*, NAT'L CONFERENCE OF STATE LEGISLATURES (Dec. 12, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx [https://perma.cc/KDW8-GDXF]. States might also utilize their own constitutional provisions to regulate police. *See, e.g.*, N.H. Const. pt. 1, art. 2-b ("An individual's right to live free from governmental intrusion in private or personal information is natural, essential, and inherent."); People v. Chapman, 679 P.2d 62, 68, 71 (Cal. 1984), *overruled on other grounds by* People v. Palmer, 15 P.3d 234 (Cal. 2001) (ruling that California's constitution expressly protects privacy and rejects the third party doctrine).

of *Katz*, enacted Title III to specify controls on "nonconsensual" interception of any wire, oral, or electronic communications.[367]

Although online privacy affects millions of individuals, the legislative sclerosis evident with privacy protections more generally will likely materialize in this arena.[368] This is especially so both because political actors are reluctant to do anything that might be interpreted as aiding criminal suspects[369] and because politically powerful Internet businesses, bent on accessing ever more data without limit, will likely mount a vigorous resistance.[370] Also, even if a legislature acts to preserve user privacy, experience teaches that exceptions will be drawn for law enforcement.[371]

A better approach, we submit, is to leverage private law—contract law in particular. As Richard Re argued in response to Baude and Stern, private law can play a privacy-defining role: it can allow individuals to protect their privacy "[b]y choosing to do business with telecoms or other companies that contractually commit to keeping customer information confidential."[372] Similar to the feedback loop we later propose,[373] Re envisions that "consumer arrangements would support expanded Fourth

367. Kerr, *New Technologies*, *supra* note 207, at 850.

368. *See, e.g.*, Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 MICH. L. REV. 485, 533–37 (2013) (noting that legislatures are often dominated by law enforcement interests and the unwillingness of legislatures to amend "obviously flawed and outdated provisions"); David Alan Sklansky, *Two More Ways Not to Think About Privacy and the Fourth Amendment*, 82 U. CHI. L. REV. 223, 230 (2015) ("We lack good examples of Congress stepping in to regulate a technological threat to privacy that the Court has left entirely unaddressed.").

369. *See, e.g.*, David Jaros, *Flawed Coalitions and the Politics of Crime*, 99 IOWA L. REV. 1473 (2014); Ronald F. Wright & Wayne A. Logan, *The Political Economy of Application Fees for Indigent Criminal Defense*, 47 WM. & MARY L. REV. 2045, 2068–71 (2006).

370. *See, e.g.*, Hannah Albarazi, *Facebook Says Social Media Users Can't Expect Privacy*, LAW360 (May 29, 2019), https://www.law360.com/articles/1164091 (describing a hearing in which Facebook's counsel argued that because users consent to sharing information "[t]here is no invasion of privacy at all, because there is no privacy").

371. Murphy, *supra* note 368, at 487 ("The United States Code currently contains over twenty separate statutes that restrict both the acquisition and release of covered information . . . . Yet across this remarkable diversity, there is one feature that all these statutes share in common: each contains a provision exempting law enforcement from its general terms.").

372. Re, *supra* note 360, at 336.

373. *See infra* notes 392–409 and accompanying text.

Amendment rights: if the government trumped those contractual duties by ordering or excusing disclosure of customer information without a warrant, then it would trigger the positive law floor's presumptive rule of unreasonableness."[374]

Despite the many benefits of our approach, identified in Part III, there are and should be some limits on the power of contract law to determine privacy rights. For example, in *Cramer v. Consolidated Freightways, Inc.*,[375] a collective bargaining agreement contained provisions permitting use of two-way mirrors in employee bathrooms, which were illegal under California privacy law. In deeming the provisions invalid, the Ninth Circuit Court of Appeals relied upon Supreme Court precedent recognizing that federal collective bargaining laws do not "grant the parties to a collective-bargaining agreement the ability to contract for what is illegal under state law."[376]

Furthermore, one might reasonably worry whether the contract model advanced here will mark an improvement over the indeterminacy of Fourth Amendment doctrine so often criticized. One might ask, for instance, whether we are simply substituting one form of judge-made normative decision-making for another.[377] Indeed, one might view with skepticism the assertion that the interpretive views of judges—given their distinct background, experience, and education—align with those of average consumers.[378]

To the extent such variability exists, and is of concern, relief might lie in definitive interpretation of commonly used boilerplate language by the highest court in a given jurisdiction. A court might benefit by adopting a proposal recently advanced by

374. Re, *supra* note 360, at 336–37.

375. *See* Cramer v. Consol. Freightways, Inc., 255 F.3d 683, 694–95 (9th Cir. 2001) (en banc).

376. *Id.* at 695 (quoting Allis-Chalmers Corp. v. Lueck, 471 U.S. 202, 212 (1985)).

377. *See, e.g.*, United States v. Jones, 565 U.S. 400, 427 (2012) (Alito, J., concurring) (acknowledging that "judges are apt to confuse their own expectations of privacy with those of the hypothetical reasonable person to which the *Katz* test looks"); Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring) (referring to *Katz* as a "self-indulgent" test and claiming that the expectations of privacy society is prepared to recognize as reasonable "bear an uncanny resemblance to those expectations of privacy that this Court considers reasonable").

378. *See, e.g.*, Verizon Directories Corp. v. Yellow Book USA, Inc., 309 F. Supp. 2d 401, 407 (E.D.N.Y. 2004) (noting distinctiveness of federal judges in terms of "background and experience").

Omri Ben-Shahar and Lior Strahilevitz to interpret contracts through the use of large population surveys.[379] In the Fourth Amendment litigation context, with the right to privacy decided pretrial by judges, survey results regarding standard form service agreements and privacy settings would be particularly useful, with findings of a privacy right (or not) having an impact on similar cases,[380] perhaps resulting in more privacy-protective agreements and firm behavior.[381]

Yet, even assuming intra-jurisdictional variability is not a concern, variation among states regarding matters such as what qualifies as an unenforceable contract of adhesion might problematically lead to variable privacy protections.[382] While these concerns are valid, this result does not differ in kind from regional variations in Fourth Amendment protections. Despite repeated assertions of the Supreme Court to the contrary,[383] it has

379. Omri Ben-Shahar & Lior Jacob Strahilevitz, *Interpreting Contracts Via Surveys and Experiments*, 92 N.Y.U. L. REV. 1753, 1758 (2017) ("Instead of asking judges and juries to interpret contracts, the meaning of disputed contractual clauses should be determined by polling a large representative sample of disinterested respondents. Let majorities of survey respondents decide. For consumer contracts . . . that entails polling a representative sample of consumers."). The authors' empirical approach aligns with prior efforts to harness public views on the intrusiveness of police behaviors to determine whether the behaviors qualify as a Fourth Amendment search. *See, e.g.*, Henry F. Fradella et al., *Quantifying* Katz*: Empirically Measuring "Reasonable Expectations of Privacy" in the Fourth Amendment Context*, 38 AM. J. CRIM. L. 289 (2011).

380. *See* Ben-Shahar & Strahilevitz, *supra* note 379, at 1806 ("Once contract language is tested and its meaning validated via surveys, it could be replicated widely within an industry.").

381. The flaw inherent in such a test is that consumers might conclude boilerplate language is always enforceable, no matter how it was presented to them, and regardless of whether the terms were fair. *See* Furth-Matzkin & Sommers, *supra* note 352; *see also* Tess Wilkinson-Ryan, *The Perverse Consequences of Disclosing Standard Terms*, 103 CORNELL L. REV. 117, 121–22 (2017) (reporting studies where respondents found terms more enforceable, despite their apparent unfairness, when embedded in unread fine print).

382. *Compare, e.g.*, Antkowiak v. TaxMasters, 455 F. App'x 156, 159–60 (3d Cir. 2011) ("Contracts of adhesion are per se procedurally unconscionable in Pennsylvania."), *with* Meyer v. State Farm Fire & Cas. Co., 582 A.2d 275, 278 (Md. Ct. Spec. App. 1990) (refusing to deem contracts of adhesion per se unconscionable), *and* Vitale v. Schering-Plough Corp., 174 A.3d 973, 980 (N.J. 2017) ("[A] contract of adhesion is not per se unenforceable."), *and* Berent v. CMH Homes, Inc., 466 S.W.3d 740, 756 (Tenn. 2015) ("[C]ontracts of adhesion are not per se unenforceable in Tennessee.").

383. *See, e.g.*, Danforth v. Minnesota, 552 U.S. 264, 302 (2008) (Roberts, C.J., dissenting) (citation omitted) (asserting that federal rights must be "applied equally" in "every one of the several States"); Mapp v. Ohio, 367 U.S. 643, 660

long been the case that search and seizure rights can and do differ considerably among jurisdictions.[384] This variability is an inevitable aspect of the nation's federalist system and has a variety of benefits, including the instantiation of state and local democratic (as opposed to federal judicial) "normative preferences."[385]

Finally, one could argue that our contract-dependent approach is problematic because it would entail *personal variability* of Fourth Amendment rights,[386] based on individuals' contractual preferences.[387] How can it be, it might be asserted, that an individual should be able to bargain for more constitutional

(1961) (stating expectation that the Fourth Amendment be "enforceable in the same manner and to like effect" nationwide); *see also* The Federalist No. 2, at 38–39 (John Jay) (Clinton Rossiter ed., 1961) ("[W]e have uniformly been one people; each individual citizen everywhere enjoying the same national rights, privileges, and protection.").

384. *See generally* Wayne A. Logan, *A House Divided: When State and Lower Federal Courts Disagree on Federal Constitutional Rights*, 90 NOTRE DAME L. REV. 235, 254–58 (2014) (identifying numerous judicial disagreements regarding Fourth Amendment search and seizure doctrine); Wayne A. Logan, *Contingent Constitutionalism: State and Local Criminal Laws and the Applicability of Federal Constitutional Rights*, 51 WM. & MARY L. REV. 143, 151–56 (2009) [hereinafter Logan, *Contingent Constitutionalism*] (noting ways in which varied state criminal laws affect Fourth Amendment doctrine).

385. *See* Logan, *Contingent Constitutionalism*, *supra* note 384, at 161–63, 172–81.

386. In a recent article, Matthew Kugler and Lior Strahilevitz urge that constitutional criminal procedure, including Fourth Amendment expectations of privacy and consent to search, be "personalized" based on broad demographic factors like race, age, and gender, informed by survey results of test subjects. Matthew B. Kugler & Lior Jacob Strahilevitz, *Assessing the Empirical Upside of Personalized Criminal Procedure*, 86 U. CHI. L. REV. 489 (2019). Their study ultimately demonstrated only small statistically significant effects. *Id.* at 508. However, they conclude that:

> A data-driven approach to personalization may look attractive in comparison to the status quo, in which judges and justices are forced to rely on their own, perhaps idiosyncratic, views about what's reasonable . . . . And we should not kid ourselves—the criminal justice system already tolerates a degree of disparate treatment across protected classes. Personalization based on race, age, and sex is not constitutionally unthinkable even though it raises hard normative questions and should generate careful constitutional scrutiny.

Id. at 517.

387. As Julie Cohen has argued, denying individuals the ability to contract for data privacy effectively denies them their autonomy, treating them "as the natural and appropriate objects of others' trades, others' choices, others' taxonomies, and others' speech." Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1377 (2000).

privacy? Indeed, under such a regime, firms might rationally seek to placate the informed minority of individuals who are aware of privacy risks, and the steps they can take to alleviate them, leaving the (comparatively benighted) marketplace majority with less protective defaults.[388]

For better or worse, however, the Supreme Court has made clear that Fourth Amendment rights are *personal rights*,[389] and that some individuals can organize and operate their lives to secure comparatively greater privacy.[390] Consider, for example, the privacy rights of those who live in single-family homes, especially with yards or property attached, compared to those who live in a multi-unit apartment building. Holding other factors constant, a home with curtilage, the area physically surrounding a home and afforded its heightened privacy protection, will provide a broader zone of privacy to its residents.[391]

Ultimately, however, we hope our model will have a salutary leveling-up effect, heightening awareness among users of the importance of agreements and settings,[392] and inducing firms to

388. *See* R. Ted Cruz & Jeffrey J. Hinck, *Not My Brother's Keeper: The Inability of an Informed Minority to Correct for Imperfect Information*, 47 HASTINGS L.J. 656, 674–75 (1996) (arguing that informed consumers may receive protections that are not afforded to an uninformed consumer). As one commentator recently put it:

> An informed minority problem poses a further problem to creating better privacy practices on social media platforms . . . . [T]hose users best educated about the privacy threats of social media use will set their privacy settings very narrowly or will not use the social media sites at all. However, the lack of transparency concerning the privacy settings of one's social media connections means that social media sites can mollify those most aware of the privacy risks while leaving the majority uninformed.

Mund, *supra* note 23, at 265 n.125; *see also* Linford, *supra* note 248, at 1421.

389. *See, e.g.*, Minnesota v. Carter, 525 U.S. 83, 88 (1998); United States v. Payner, 447 U.S. 727, 731–32 (1980); *cf.* Jay P. Kesan, *Cyber-Working or Cyber-Shirking?: A First Principles Examination of Electronic Privacy in the Workplace*, 54 FLA. L. REV. 289, 293 (2002) (arguing for a "market-based, contractarian" approach to providing employees of private companies a right to electronic privacy in the workplace).

390. *See* Wayne A. Logan, *Fourth Amendment Localism*, 93 IND. L.J. 369, 376–82 (2018) (explaining Fourth Amendment variations based inter alia upon local laws, geography, and public resources).

391. Jake Linford, Comment, *The Right Ones for the Job: Divining the Correct Standard of Review for Curtilage Determinations in the Aftermath of* Ornelas v. United States, 75 U. CHI. L. REV. 885, 886 (2008).

392. One way of doing so might be by "personalization" of privacy notices,

modify their behavior in a privacy-protective direction.[393] Facing market pressure, ideally firms will embrace the opportunity to compete on privacy,[394] improving website designs to increase user understanding and choice;[395] augment the granularity and user-friendliness of privacy settings;[396] enhance the readability

which could utilize algorithmic data on individuals to customize their data sharing preferences. Christoph Busch, *Implementing Personalized Law: Personalized Disclosures in Consumer and Data Privacy Law*, 86 U. CHI. L. REV. 309, 319–22 (2019).

393. More broadly, with users more sensitized to the privacy consequences of their online lives, there is also hope that firms will be more transparent about their monitoring and gathering of users' information. It was recently revealed, for instance, that popular iPhone apps—without any notice in their privacy policies—have been taking screen shots of users' phones, ostensibly to discern how they interact with apps, but for the firms' analytic benefit, and risking exposure of users' sensitive information, such as banking and passcode information. Zack Whittaker, *Many Popular iPhone Apps Secretly Record Your Screen Without Asking*, TECHCRUNCH (Feb. 6, 2019, 4:35 PM), https://techcrunch.com/2019/02/06/iphone-session-replay-screenshots/ [https://perma.cc/9Q8S-TDTQ]. In response, Apple told app developers to discontinue or properly disclose their use of the analytics code or face removal from the Apple app store. Zack Whittaker, *Apple Tells App Developers to Disclose or Remove Screen Recording Code*, TECHCRUNCH (Feb. 7, 2019, 3:43 PM), https://techcrunch.com/2019/02/07/apple-glassbox-apps/ [https://perma.cc/EQ5J-6TNQ].

394. *See, e.g.*, Kesan et al., *supra* note 223, at 269 ("Partly in response to public concern over government surveillance, Apple and Google announced in late 2014 that their future products will, by default, use extremely strong encryption that even the companies themselves could not bypass."). Indeed, Steven Hetcher argues that concern about information privacy is a recent phenomenon, rising to prominence because of privacy advocates whose efforts shifted website norms in the early twentieth century. Steven Hetcher, *Changing the Social Meaning of Privacy in Cyberspace*, 15 HARV. J.L. & TECH. 149, 161–62 (2001).

395. As two privacy researchers recently suggested, "[p]rivacy awareness tools should empower users to make well-informed decisions with regard to their information disclosure. Furthermore, interface design should bring attention to such intentions in terms of mobilization (activating heuristics which protect the user)." Barth & de Jong, *supra* note 289, at 1051; *see also, e.g.*, Lilian Edwards & Ian Brown, *Data Control and Social Networking: Irreconcilable Ideas?*, *in* HARBORING DATA: INFORMATION SECURITY, LAW, AND THE CORPORATION 19 (Andrea M. Matwyshyn ed., 2009); Waldman, *Privacy, Notice, and Design*, *supra* note 278 (noting improvements that can be made to enhance privacy rights); Wu, *supra* note 292, at 210 (reporting on studies that "reveal the complexity of identifying subsets of friends when sharing. [The] findings raise the question about the extent to which those [privacy settings] capture the users' real privacy preferences."); *id.* at 214 ("The one-size-fits-all privacy settings may result in . . . 'context collapse,' where privacy-sensitive contexts are not distinguished in access control mechanisms.").

396. *See* Kayes & Iamnitchi, *supra* note 234, at 3–5 (urging the inclusion of

of agreements;[397] and eschew manipulative and even fraudulent practices now common among providers.[398] Such improvements are especially important given the wide range of relative sophistication and privacy savviness known to exist among Internet users.[399]

The shift, in short, would remedy what has been a notable market failure between what consumers expect or think they are getting regarding online privacy,[400] and what firms actually deliver.[401] Currently, social media firms make black box decisions that they feel obliged to reconsider only when social outrage reaches a sufficient level.[402]

---

user options allowing for greater granularity in privacy control management). Kayes and Iamnitchi note that the current widespread use of default settings among users, and accompanying under-utilization of privacy offerings, "[is] mostly due to poor privacy setting interface, intricate privacy settings, and inherent trust in [online social networks]. The problem with not changing the default settings is that they almost always tend to be more open than users would prefer." *Id.* at 6.

397. *See, e.g.*, Uri Benoliel & Shmuel I. Becher, *The Duty to Read the Unreadable*, 61 B.C. L. REV. (forthcoming 2019); McNealy, *supra* note 234.

398. *See, e.g.*, Reidenberg et al., *supra* note 277, at 87–88; Waldman, *Privacy, Sharing, and Trust*, *supra* note 313, at 232.

399. *See* Mary Graw Leary, *Reasonable Expectations of Privacy for Youth in a Digital Age*, 80 MISS. L.J. 1035, 1039 (2011) (noting distinction drawn between "digital natives" and "digital immigrants").

400. *See, e.g.*, Hichang Cho et al., *Optimistic Bias About Online Privacy Risks: Testing the Moderating Effects of Perceived Controllability and Prior Experience*, 26 COMPUTERS HUM. BEHAV. 987 (2010) ("[I]ndividuals display a strong optimistic bias about online privacy risks, judging themselves to be significantly less vulnerable than others to these risks."); Young Min Baek et al., *My Privacy is Okay, but Theirs is Endangered: Why Comparative Optimism Matters in Online Privacy Concerns*, 31 COMPUTERS HUM. BEHAV. 48 (2014) ("[U]sers tend to believe privacy infringement is less likely to happen to oneself than to others."). Aggravating matters, users often overestimate their technological abilities in their privacy management. *See supra* note 312 and accompanying text.

401. *See* Grimmelmann, *Saving Facebook*, *supra* note 233, at 1178–79. Grimmelmann explains:

> The problem is that there's a consistent difference between how much privacy users expect when they sign up for a social network site and how much they get. That's a market failure; if users overestimate how much privacy they'll get, they won't negotiate for enough, and companies will rationally respond by undersupplying it. In order to have a well-functioning market for social network sites there would need to be a feedback loop; instead, there's a gap.

Id.

402. Jennifer Grygiel & Nina Brown, *Are Social Media Companies Motivated*

Facebook and its family of social networking platforms, which dominate the online environment, have signaled their desired shift toward facilitation of more private interactions among users, creating a "digital living room," where "people could expect their discussions to be intimate, ephemeral and secure from outsiders."[403] If and when this occurs, there will come a much-needed alignment of the "notice and choice"[404] approach to online privacy with user desires and marketplace realities,[405] in keeping with modern data protection laws predicated on a model of

to be Good Corporate Citizens? Examination of the Connection Between Corporate Social Responsibility and Social Media Safety, 43 TELECOMM. POL'Y 445 (2019) (arguing that it is rational but problematic that firms reconsider policies following social pressure); Joel Schectman, *Facebook Releases New Privacy Safeguards After Ceding to Pressure from Advertisers*, REUTERS (June 13, 2018, 10:11 AM), https://www.reuters.com/article/us-facebook-privacy-broker/facebook-releases-new-privacy-safeguards-after-ceding-to-pressure-from-advertisers-idUSKBN1J924P [https://perma.cc/J6NQ-C3MX].

403. Mike Isaac, *Mark Zuckerberg Says He'll Shift Focus to Users' Privacy*, N.Y. TIMES (Mar. 6, 2019), https://www.nytimes.com/2019/03/06/technology/mark-zuckerberg-facebook-privacy.html. In his new "Privacy-focused Vision for Social Networking," Facebook CEO Mark Zuckerberg noted the continued importance of "[p]ublic social networks," but wrote that:

> with all the ways people also want to interact privately, there's also an opportunity to build a simpler platform that's focused on privacy first
>
> . . . .
>
> People should have simple, intimate places where they have clear control over who can communicate with them and confidence that no one else can access what they share
>
> . . . .
>
> I believe we should be working towards a world where people can speak privately and live freely knowing that their information will only be seen by who they want to see it and it won't all stick around forever.

Read Mark Zuckerberg's Blog Post on His "Privacy-Focused Vision" for Facebook, N.Y. TIMES (Mar. 6, 2019), https://www.nytimes.com/2019/03/06/technology/facebook-privacy-blog.html. *But see* Zeynep Tufekci, *Zuckerberg's So-Called Shift Toward Privacy*, N.Y. TIMES (Mar. 7, 2019), https://www.nytimes.com/2019/03/07/opinion/zuckerberg-privacy-facebook.html ("[T]he few genuinely new steps that Mr. Zuckerberg announced on Wednesday seem all too conveniently aligned with Facebook's needs, whether they concern government regulation, public scandal or profitability.").

404. Barrett, *supra* note 316, at 8; Reidenberg et al., *supra* note 277, at 42–46.

405. *See* Tokson, *supra* note 233, at 150 ("[Courts] generally look to what a person *should* know, rather than what she actually did know . . . . [C]ourts do this by reaching a conclusion about the collective knowledge possessed by society and then imputing that knowledge to the person at issue."); *see also id.* at 171 ("Courts' failure to recognize the complex, multilevel nature of knowledge

privacy "self-management."[406] And, unlike the one-way ratchet resulting from application of the traditional *Katz* test,[407] courts applying the approach advocated here would push the reasonable expectation of online privacy in a more privacy-protective direction,[408] expanding privacy in a virtuous feedback loop as firms respond to consumer demand.[409]

CONCLUSION

Our goal here has been both descriptive and prescriptive. Descriptively, we highlighted a phenomenon that has gone largely unnoticed: state and lower federal courts have been reshaping the third party doctrine, which denies individuals a Fourth Amendment expectation of privacy in information they voluntarily disclose to others. The courts have done so when deciding privacy claims brought by individuals who have shared their information online, often basing their decisions in significant part on users' privacy settings and the terms of service agreements.

Prescriptively, building upon this foundation, we have advocated a model making fuller use of contract law. We urge applying contract law's interpretive tools to assess the privacy effect of user agreements, website design, and privacy settings, informed by research regarding the real-world contexts in which

often leads them to find that people have knowingly waived their Fourth Amendment rights on very thin evidence.").

406. *See generally* Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880 (2013) ("[T]he law provides people with a set of rights to enable them to make decisions about how to manage their data.").

407. *See* Jim Harper, *Reforming Fourth Amendment Privacy Doctrine*, 57 AM. U. L. REV. 1381, 1382 (2008) (noting the practical effect of Justice Harlan's concurring opinion in *Katz*); Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1519 (2010) ("[T]he [*Katz*] test has failed to live up to aspirations.").

408. Federal agencies, such as the Federal Trade Commission, could also play a useful role in hastening such improvements. Solove & Hartzog, *supra* note 317, at 627–66. State legislatures can also enact statutes that protect consumers with weaker bargaining power from waiving rights by requiring that waivers be "voluntary and knowing" or imposing limitations like waiting periods or rescission periods, to increase certainty that individuals knowingly waive their rights. Jessica Wilen Berg, *Understanding Waiver*, 40 HOUS. L. REV. 281, 342 (2003).

409. *See* Alan Schwartz & Louis L. Wilde, *Intervening in Markets on the Basis of Imperfect Information: A Legal and Economic Analysis*, 127 U. PA. L. REV. 630, 638–39 (1979).

they are operationalized. Ultimately, we concluded that contracts doctrine has much to offer Fourth Amendment privacy analyses, certainly compared to the indeterminacy of the *Katz* status quo and other recently advanced alternatives.[410] Taking their cue from the Supreme Court, as courts shift away from the traditional zero-sum privacy orientation of the third party doctrine when assessing online privacy questions, contract tools of interpretation can and should help determine outcomes.

Given the integral role the internet has come to play in our social, political, and economic lives,[411] the task we have undertaken is as timely as it is important. It took forty years for the Supreme Court in *Katz* to recognize what was true when *Olmstead* was decided: "To read the Constitution [too] narrowly is to ignore the vital role that the public telephone has come to play in private communication."[412] Our hope is that contracts doctrine, a well-established cornerstone of private law ordering, already used by the Supreme Court to inform privacy rights in some contexts, can assume a more prominent role in determining reasonable expectations of privacy in the Internet Age.

410. As a result, private law will affect Fourth Amendment online privacy in much the same way it has come to affect First Amendment online free speech and association. *See* Jacquelyn E. Fradette, Note, *Online Terms of Service: A Shield for First Amendment Scrutiny of Government Action*, 89 NOTRE DAME L. REV. 947, 956–57 (2013).

411. *See supra* notes 5, 73–75, and accompanying text; *see also, e.g.*, Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 923–24 nn.7–8 (2005) (citing studies discussing the social importance of online relationships and information sharing).

412. Katz v. United States, 389 U.S. 347, 352 (1967).