Minnesota Journal of Law, Science & Technology

Volume 21 | Issue 1 Article 5

5-27-2020

The Indiscretion of Friends: Fourth Amendment Concerns About the Ability to Predict a Person's Online Social Activity by Monitoring Her Contacts

George M. Dery III

Follow this and additional works at: https://scholarship.law.umn.edu/mjlst

 Part of the Constitutional Law Commons, Criminal Procedure Commons, Fourth Amendment Commons, and the Internet Law Commons

Recommended Citation
George M. Dery III, *The Indiscretion of Friends: Fourth Amendment Concerns About the Ability to Predict a Person's Online Social Activity by Monitoring Her Contacts*, 21 MINN. J.L. SCI. & TECH. 137 (2019).
Available at: https://scholarship.law.umn.edu/mjlst/vol21/iss1/5

The Minnesota Journal of Law, Science & Technology is published by the University of Minnesota Libraries Publishing.

The Indiscretion of Friends: Fourth Amendment Concerns About the Ability to Predict a Person's Online Social Activity by Monitoring Her Contacts

George M. Dery III*

ABSTRACT:

This Article considers new predictive surveillance technology that could enable social media companies, as well as law enforcement agencies, to predict a person's future behavior based solely on an examination of the person's contacts. Employing the tools of information theory, scientists at the University of Vermont and the University of Adelaide have been able to predict Twitter users' future behavior by scrutinizing only the responses of their contacts. This technological advance, which can be applied to other kinds of social media, raises the prospect of law enforcement gaining insight into the future behavior of social media users even if such targets choose to withdraw from social media. This Article analyzes the strength of potential arguments for Fourth Amendment protection against this possibility. If subjects of predictive surveillance argue that communications with their contacts should be off limits to law enforcement, precedent regarding disclosures by confidants to police indicates these contentions will likely fail. However, the "target" theory of standing, previously rejected by the Supreme Court, might allow claims of Fourth Amendment violations in the unique context of predictive surveillance. Finally, the strongest argument for protection against government scrutiny of contacts to predict a person's future social media behavior would combine the Fourth

---

© 2020 George M. Dery III

* Professor, California State University Fullerton, Division of Politics, Administration, and Justice; Former Deputy District Attorney, Los Angeles, California; J.D., Loyola Law School, Los Angeles, 1987; B.A., University of California Los Angeles, 1983. The author would like to thank his colleague, Dr. Dixie Koo, for her thoughtful and helpful advice on this article.

Amendment rights of a homeowner with recent Court rulings extending privacy protection to digital information.

Abstract:.....137
I. Introduction 139
II. Defining a Fourth Amendment "Search" 141
III. Predicting a Person's Activity Simply by Studying Her Social Media Contacts.....142
IV. Potential Arguments for Fourth Amendment Privacy Protection Against the Predictive Surveillance of Anticipating a Social Media User's Behavior by Monitoring Her Contacts 145
A. Subjects of Predictive Surveillance Will Likely Be Unable to Argue Fourth Amendment Privacy for Communications with Friends Since the Supreme Court Has Repeatedly Refused to Protect Disclosures Made by Friends.....145
B. A Former User of Social Media Claiming Fourth Amendment Privacy Against Government Exploitation of Her Contacts Could Resurrect "Target" Standing as Particularly Apt for Predictive Surveillance 150
C. A Reinterpretation of Court Precedent Regarding a Homeowner's Right to Privacy, when Viewed with Court Rulings on Collection of Digital Information, Could Provide the Strongest Argument for Fourth Amendment Protection Against Predictive Surveillance of Social Media 154
V. Conclusion.....167

I. INTRODUCTION

Have you grown weary of the privacy invasions of social media? Perhaps you were appalled by Facebook's collection of "sensitive personal information about sexual orientation, race, gender, even intelligence and childhood trauma" from some of its users.[1] Maybe you were alarmed by the proposed $5.3 million settlement by such Internet giants as Instagram, Twitter, and Yelp regarding a privacy lawsuit.[2] After such revelations, the prudent course might be to simply opt out of social media. The loss of connections, updates, and entertainment, however isolating, would be the necessary cost of preserving your privacy. While such a decision might be wise and even laudable, it would also come too late.

Researchers from the University of Vermont and the University of Adelaide report that limiting the use of social media and even completely deleting accounts provide "no guarantee of privacy."[3] Employing "tools from information theory," James P. Bagrow, Xipei Liu, and Lewis Mitchell were able to "repeatedly and accurately predict the text" of Twitter users by focusing only on the "social ties" of a user, rather than accessing the user's own data.[4] Essentially, these computer scientists have demonstrated that "the Twitter streams of your [ten] closest contacts can predict your future tweets even better than your own stream."[5] Further, even though this particular research focused on Twitter, Bagrow warned, "the same information could be gathered from posts on other social media,

---

1. Carole Cadwalladr & Emma Graham-Harrison, *How Cambridge Analytica Turned Facebook 'Likes' into A Lucrative Political Tool*, THE GUARDIAN (Mar. 17, 2018, 9:02 AM), https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm.

2. Jeff J. Roberts, *Instagram, Twitter, and Others Could Pay Users $5.3 Million in App Privacy Settlement*, FORTUNE (Apr. 4, 2017, 10:53 PM), http://fortune.com/2017/04/04/find-friends-privacy-instagram-twitter/.

3. Matthew Hutson, *People Can Predict Your Tweets—Even If You Aren't on Twitter*, SCI. (Jan. 21, 2019, 11:00 AM), https://www.sciencemag.org/news/2019/01/people-can-predict-your-tweets-even-if-you-aren-t-twitter.

4. James P. Bagrow, Xipei Liu & Lewis Mitchell, *Information Flow Reveals Prediction Limits in Online Social Activity*, 3 NATURE HUM. BEHAV. 122, 126 (2019).

5. Hutson, *supra* note 3.

like Facebook."[6] Bagrow's coauthor, Lewis Mitchell, simply said, "There's no place to hide in a social network."[7]

The prospect of social media companies or law enforcement being able to build predictive profiles based solely on one's contacts has troubling Fourth Amendment implications.[8] Can any person reasonably expect privacy when using social media, or even after leaving such platforms, when "a person's choices and identity are embedded" in these social media services?[9] Must Fourth Amendment protection be simply abandoned as part of the price of functioning in a "highly networked society[?]"[10]

This Article reviews Supreme Court precedent to consider arguments that the Fourth Amendment protects against predictive surveillance by law enforcement of social media contacts in order to divine the future behavior of a user or former user. The prior case law indicates that while some contentions will not convince the Court, others could present a path to Fourth Amendment protection for those using social media. This Article begins, in Part II, with a review of the Court's definition of a Fourth Amendment "search." Part III provides an examination of the technology behind predictive surveillance. Finally, Part IV analyzes the strength of the potential arguments advocating for Fourth Amendment protection from this new technology. If those subject to predictive surveillance argue that their communications with friends and other contacts should be off-limits to law enforcement, precedent regarding disclosures by friends to police would indicate these contentions likely fail. However, the "target" theory of standing, previously rejected by the Court, might allow claims of Fourth Amendment

---

6. Umberto Bacchi, *'No Place to Hide': Twitter Contacts Give Your Preferences Away, Study Finds*, THOMSON REUTERS FOUND. (Jan. 21, 2019, 6:59 PM), http://news.trust.org/item/20190121185119-yg73i/.

7. *Id*.

8. *See* U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

9. Joshua E. Brown, *Study: On Facebook and Twitter Your Privacy Is at Risk—Even If You Don't Have an Account*, UVM TODAY (Jan. 21, 2019), https://www.uvm.edu/uvmnews/news/study-facebook-and-twitter-your-privacy-risk-even-if-you-dont-have-account.

10. *Id*.

violations in the unique context of predictive surveillance. Finally, the strongest argument might combine the Fourth Amendment rights of a homeowner with recent Court rulings extending privacy protection to digital information.

II. DEFINING A FOURTH AMENDMENT "SEARCH"

As with any law, the Fourth Amendment can only be violated if it applies in the first place. By its own terms, the Fourth Amendment applies only to "searches and seizures."[11] The Court provided a definition of a Fourth Amendment "search" in *Katz v. United States*, a case in which federal agents placed "an electronic listening and recording device to the outside of the public telephone booth" from which Katz placed a phone call.[12] This electronic device enabled the government to collect Katz's side of a conversation in which he illegally transmitted "wagering information" in violation of federal law.[13] The Court ruled that the agents' "activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth" and therefore amounted to a Fourth Amendment "search."[14]

Katz supported its conclusion with ringing language, declaring that "the Fourth Amendment protects people, not places."[15] The Court proclaimed, "Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures."[16] Recognizing "the vital role that the public telephone has come to play in private communication," *Katz* concluded that anyone who occupies a phone booth "shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[17]

---

11. U.S. CONST. amend. IV.

12. Katz v. United States, 389 U.S. 347, 348 (1967). *But see* United States v. Jones, 565 U.S. 400, 404–05 (2012) (recognizing when the government "physically occupie[s] private property for the purpose of obtaining information" as a second definition of a Fourth Amendment search). Since the technology analyzed in this article will not necessitate such a physical trespass, *Jones'* definition is beyond the scope of this article. Further, analysis of Fourth Amendment "seizures" is also beyond the scope of this article.

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

14. *Id.* at 353.

15. *Id.* at 351.

16. *Id.* at 359.

17. *Id.* at 352.

The *Katz* court spoke in such broad strokes that it provided few specifics for a workable rule. Justice Harlan, in his concurrence, wrote separately to address this problem. He noted: "As the Court's opinion states, 'the Fourth Amendment protects people, not places.'"[18] The Court's declaration, however, left unanswered "what protection" the Fourth amendment "affords to those people."[19] Justice Harlan proposed the following clarifying guidance: "My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[20] For example, "a man's home is, for most purposes, a place where he expects privacy."[21] In contrast, "conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable."[22] Following Justice Harlan's formulation, the "Court uniformly has held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action."[23] Indeed, the Court would come to label *Katz*'s definition of a Fourth Amendment search as its "touchstone."[24]

III. PREDICTING A PERSON'S ACTIVITY SIMPLY BY STUDYING HER SOCIAL MEDIA CONTACTS

Bagrow, Liu, and Mitchell considered the feasibility of predicting a Twitter user's future communications by analyzing her closest contacts' tweets.[25] They began their "second-hand surveillance"[26] of people's online behavior by randomly sampling

---

18. *Id.* at 361 (Harlan, J., concurring).
19. *Id.*
20. *Id.*
21. *Id.*
22. *Id.*
23. Smith v. Maryland, 442 U.S. 735, 740 (1979).
24. Oliver v. United States, 466 U.S. 170, 177 (1984).
25. *See generally* Bagrow, Liu & Mitchell, *supra* note 4 at 122 (using "information theoretic tools to estimate the predictive information in the writings of Twitter users").
26. Hutson, *supra* note 3.

Twitter during April 2014.[27] The researchers sampled 927 Twitter users who tweeted in English, had been active for "at least a [one]-year period[,]" and who had "50 [to] 500 followers."[28] The cutoff of those accounts below fifty followers avoided "inactive and bot accounts" while the cutoff above 500 followers steered clear of "unusually popular" outliers "such as celebrity accounts."[29] The scientists collected all of the "public postings," excluding retweets, of their 927 users, whom they labeled as "egos."[30] An examination of these tweets enabled the researchers to identify their 927 egos' top fifteen Twitter followers.[31] The researchers, deeming these 13,905 followers as "alters," gathered their tweets as well.[32]

The researchers aimed to predict the written text of their 927 egos, noting that "[r]epeated, accurate predictions of future words indicate that the available information can be used to build profiles and predictive models of a user."[33] In estimating "how predictable a person's future words would be," the researchers used "a measurement known as entropy."[34] Entropy can limit predictability because "more entropy means more randomness and less repetition."[35] To put the Twitter users' entropy rates in context, the researchers measured the entropy rates of writing in "formal text," such as that of Ernest Hemingway and James Joyce.[36] "On [a]verage," the 927 Twitter users "had more entropy than Ernest Hemingway" and "less

---

27. Bagrow, Liu & Mitchell, *supra* note 4, at 126.

28. *Id*.

29. *Id*.

30. *Id*. at 122.

31. *See id*. ("Each of the n=927 ego-networks consisted of one user (the ego) and their [fifteen] most frequently mentioned Twitter contacts (the alters) . . . .").

32. *Id*.

33. *Id*. at 123. The study's authors explain that "[t]he ability . . . to accurately profile [and predict] individuals . . . is reflected in the predictability of their written text."). *Id* at 126.

34. Hutson, *supra* note 3.

35. *Id*.

36. *Id*. The scientists measured Hemingway's *For Whom the Bell Tolls* and Joyce's *Ulysses*. They also measured the entropy rates of Thomas Pynchon's *Gravity's Rainbow* and J.R.R. Tolkien's *The Fellowship of the Ring*. James P. Bagrow, Xipei Liu, & Lewis Mitchell, *Supplementary Information for "Information Flow Reveals Prediction Limits in Online Social Activity"* at Supplementary Table 1, https://bagrow.com/pdf/information-flow-reveals-bagrow-2019_supp.pdf.

than James Joyce."[37] The study's authors then combined the entropy measurement with "a tool from information theory called Fano's inequality" to "calculate how well a person's stream could predict the first word in his or her next tweet."[38] In considering the user/ego's tweets, the upper boundary on accuracy "for predicting a given word out of (approximately) 5000 possible words on average" was about fifty-three percent which the researchers deemed "quite high."[39]

The researchers then assessed the predictability of a user's next word when considering both the user/ego's Twitter stream and the streams of the user's fifteen closest contacts/alters.[40] The predictability when considering both the user and her contacts rose to sixty percent.[41] When the user's stream was removed, leaving the researchers with only the contacts'/alters' streams to use as a basis of prediction, predictability dropped to fifty-seven percent.[42] Importantly, the accuracy obtained by using the contacts' tweets alone was greater than that obtained by simply observing the ego's tweets. Bagrow noted: "Paradoxically, this indicated that there is potentially more information about the ego within the total set of alters than within the ego itself."[43]

The study's authors thus found that "meaningful predictive information about individuals is encoded in their social ties."[44] The researchers declared, "there is so much social information that an entity with access to all social media data" will have only slightly less predictive ability when having access to a person's Twitter contacts than with access to both those contacts and the user herself.[45] The investigators explicitly warned that their work "may have distinct implications for privacy" because "if an individual forgoes using a social media platform or deletes their account, yet their social ties remain, then that platform owner potentially still possesses 95.1±3.36% of the achievable predictive accuracy of the future activities of that individual."[46]

---

37. Hutson, *supra* note 3.
38. *Id*.
39. Bagrow, Liu & Mitchell, *supra* note 4, at 123. Hutson, *supra* note 3.
40. Hutson, *supra* note 3.
41. *Id*.
42. *Id*.
43. Bagrow, Liu & Mitchell, *supra* note 4, at 124.
44. *Id.* at 122.
45. *Id*. at 125.
46. *Id*.

Bagrow has sounded the alarm, noting, "[w]hat concerns me in terms of privacy . . . is that there are so many ways that [social media] platforms are getting at data that I think people don't realize."[47] Joanne Hinds, a psychologist at the University of Bath in the United Kingdom, has asserted, "[w]e have barely scratched the surface of what types of information can be revealed" through contacts.[48] The University of Vermont, on its website, went so far as to state that "privacy on social media is like second-hand smoke. It's controlled by the people around you."[49] Privacy on social media is therefore no longer within the control of the individual. As Bagrow warned, "[y]ou alone don't control your privacy on social media platforms, . . . [y]our friends have a say too."[50]

IV. POTENTIAL ARGUMENTS FOR FOURTH AMENDMENT PRIVACY PROTECTION AGAINST THE PREDICTIVE SURVEILLANCE OF ANTICIPATING A SOCIAL MEDIA USER'S BEHAVIOR BY MONITORING HER CONTACTS

A. SUBJECTS OF PREDICTIVE SURVEILLANCE WILL LIKELY BE UNABLE TO ARGUE FOURTH AMENDMENT PRIVACY FOR COMMUNICATIONS WITH FRIENDS SINCE THE SUPREME COURT HAS REPEATEDLY REFUSED TO PROTECT DISCLOSURES MADE BY FRIENDS

People seeking Fourth Amendment protection from predictive surveillance online must first overcome a profound stumbling block—the fact that they have undermined their own privacy by involving themselves in social media in the first place. *Katz*, the "lodestar" guiding the Court's perception of privacy,[51] held, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[52] There is a sense, however, that what one confides to a friend should be kept secret. Indeed, one of the hallmarks of friendship is the ability to unburden oneself to a friend, knowing

47. Hutson, *supra* note 3.
48. *Id*.
49. Brown, *supra* note 9.
50. *Id*.
51. Smith v. Maryland, 442 U.S. 735, 739 (1979).
52. Katz v. United States, 389 U.S. 347, 351 (1967) (citing Lewis v. United States, 385 U.S. 206, 210 (1966); United States v. Lee, 274 U.S. 559, 563 (1927)).

that any indiscretion discussed is safely sealed within the bounds of that private relationship.

The Court does not share this view of friendship. It has ruled that the act of sharing information, even with one's friend, destroys the privacy of the shared secret.[53] The Court considered the privacy among old acquaintances in *On Lee v. United States*, a case in which Chin Poy, a former employee, visited On Lee's laundry for a chat.[54] Unaware that Chin Poy, armed with a microphone, was operating as an undercover agent for the Narcotics Bureau, On Lee made incriminating statements.[55] When these admissions were later offered against him, On Lee argued that they must be suppressed as obtained in violation of the Fourth Amendment.[56] The Court disagreed, finding no Fourth Amendment violation because On Lee "was talking confidentially and indiscreetly with one he trusted, and he was overheard."[57] Chin Poy's use of technology, here a radio transmitter to broadcast On Lee's statements, made privacy among co-criminals no less of a "spurious libert[y]."[58] Thus, government use of technology did not provoke Fourth Amendment protection from a false friend.[59]

The Court again denied protection for statements improvidently shared with colleagues in *Hoffa v. United States*.[60] In *Hoffa*, Teamsters Union President Jimmy Hoffa openly spoke of bribing jurors in front of Ed Partin, a union official who Hoffa had invited into his hotel room, the hotel lobby, and the

---

53. *See* On Lee v. United States, 343 U.S. 747, 753–54 (1952) (holding no Fourth Amendment violation when agent Lee overheard Petitioner talking "confidentially and indiscreetly with one he trusted," even though agent Lee overheard with the help of a transmitter and receiver).

54. *Id*. at 749.

55. *Id*.

56. *Id*. at 750.

57. *Id*. at 753–54.

58. *Id*. at 754.

59. *See id*. at 754 (refusing to treat the use of transmitter and radio as wiretapping and, ultimately, finding no Fourth Amendment violation). *See also id*. ("The use of bifocals, field glasses or the telescope to magnify the object of a witness' vision is not a forbidden search or seizure, even if they focus without his knowledge or consent upon what one supposes to be private indiscretions.").

60. *See* Hoffa v. United States, 385 U.S. 293, 302 (1966) (holding no Fourth Amendment violation because Petitioner "was not relying on the security of the hotel room; he was relying upon his misplaced confidence that Partin would not reveal his wrongdoing").

courthouse.[61] When Partin later testified at Hoffa's juror tampering trial as to what he heard while undercover,[62] Hoffa claimed such evidence was gathered in violation of the Fourth Amendment.[63] In considering Hoffa's contention, the Court waxed philosophical: "The risk of being . . . betrayed by an informer or deceived as to the identity of one with whom one deals is probably inherent in the conditions of human society. It is the kind of risk we necessarily assume whenever we speak."[64] The Court further noted: "Partin was in the suite by invitation, and every conversation which he heard was either directed to him or knowingly carried on in his presence."[65] Since Hoffa had therefore simply formed a "misplaced belief" that his hearer would not reveal his wrongdoing, he had "no interest legitimately protected by the Fourth Amendment" in the case.[66]

The Court, once again, refused Fourth Amendment protection to statements made to a government informant in *United States v. White*.[67] In *White*, Harvey Jackson met with the suspect and broadcast their conversations to government agents by radio.[68] One meeting between Jackson and White occurred in White's residence.[69] Sharing confidences, even in one's own home, did not persuade the Court to find a reasonable expectation of privacy in these communications because, "however strongly a defendant may trust an apparent colleague," such beliefs "are not protected by the Fourth Amendment when it turns out that the colleague is a government agent regularly communicating with the authorities."[70] *White* declared that anyone considering an illegal act "must realize and risk that his companions may be reporting

---

61. *Id*. at 295–96. *See also id*. at 296 n.3 ("Hoffa explained [to Partin] 'that they was going to get to one juror or try to get to a few scattered jurors and take their chances.'").

62. *Id*. at 296 n.3.

63. *Id*. at 300.

64. *Id*. at 303 (citing Lopez v. United States, 373 U.S. 427, 465 (1963) (Brennan, J., dissenting)).

65. *Id*. at 302.

66. *Id*.

67. United States v. White 401 U.S. 745 (1971).

68. *Id*. at 746–47.

69. *Id*. at 747.

70. *Id*. at 749.

to the police."[71] If the would-be wrongdoer "has no doubts, or allays them, or risks what doubt he has, the risk is his."[72]

The guidance that *On Lee*, *Hoffa*, and *White* offer to those who use social media is not entirely clear. In one sense, Twitter and Facebook users are in a weaker position than the defendants in the false friends cases. Whether seen as friends, acquaintances, or criminal colleagues, the suspects in *On Lee*, *Hoffa*, and *White* shared information with another person believing that any confidence would remain private. In contrast, those on social media are purposely posting information for others—whether friends or the general public—to consume. If the Court would not extend Fourth Amendment protection to incriminating statements uttered face-to-face behind the closed doors of the home, it certainly will not safeguard communications broadcast on the Internet.

However, predictive surveillance might result in an intrusion beyond that suffered in *On Lee*, *Hoffa*, and *White* because it collects information on future communications based on previous contacts.[73] Social media users would not have the option of avoiding further privacy invasion by simply ending a conversation or refusing a friend her next entry into the home.[74] Even if a Twitter or Facebook user blocks or un-friends someone, or chooses to leave the social media platform entirely, the government could employ predictive surveillance to collect information foretelling the user's future behavior.[75]

Further, language in *White* could offer a new tack to take in these cases. The *White* Court noted that the Court of Appeals in its case had "understood *Katz* to render inadmissible against White the agents' testimony concerning conversations that Jackson broadcast to them."[76] Rejecting the Court of Appeals' reasoning, the Court refused to equate the surveillance in *Katz* to that of *White* because, "*Katz* involved no revelation to the

---

71. *Id*. at 752.

72. *Id*.

73. *See* Bagrow, Liu & Mitchell, *supra* note 4, at 125 ("As few as 8–9 of an individual's contacts are sufficient to obtain predictability compared with that of the individual alone.").

74. *See id*. at 122 (arguing that the model presented can accurately "profile" individuals based solely off previous contacts, without any current data on the person).

75. *See id*. at 123 (presenting data showing "[r]epeated, accurate predictions of a future words . . . ").

76. United States v. White, 401 U.S. 745, 749 (1971).

Government by a party to conversations with the defendant."[77] *White* rejected the contention that anyone had a reasonable privacy expectation that "a person with whom he is conversing will not then or later reveal the conversation to the police."[78] With the advent of predictive surveillance, a social media user's contacts, of course, do indeed make "revelations" to the police about the user's future behavior simply by responding to the user's posts. The revelations, however, are made without the intention presupposed by the *White* Court. Chin Poy, Ed Partin, and Harvey Jackson deliberately collected their respective conversations, intending to directly relay them to the government. No such intentional collection would exist in the case of predictive surveillance.[79] One might need to reasonably assume the risk that the person to which one shares a confidence might choose, for her own reasons, to purposely share this information with the police.[80] However, a social media user might not reasonably be expected to weigh the risk that her contacts' usual interactions on social media would leave a mathematical trace that the government could use to divine future conduct.

The potential persuasiveness of such reasoning is open to question. Ultimately, anyone seeking Fourth Amendment protection against predictive surveillance of social media would come up against decades of precedent in which the Court has consistently held that confidences to friends and acquaintances are not protected.[81] In the past, government technology sophisticated enough to foil a suspect's calculations in assuming risk, such as wearing a wire, did not change the Court's rulings.[82] Thus, those using social media will likely receive no protection from *On Lee*, *Hoffa*, and *White*.

---

77. *Id.*

78. *Id.*

79. *See* On Lee v. United States, 343 U.S. 747, 749 (1952) (describing Chin Poy as an "undercover agent" for the Bureau of Narcotics); Hoffa v. United States, 385 U.S. 293, 296 (1966) (noting Ed Partin was a police informant); *see also White*, 401 U.S. at 746–47 (referring to Harvey Jackson as a "government informant").

80. *See Hoffa*, 385 U.S. at 303 (affirming that people assume the risk that their close confidants might become a police informant).

81. The Court decided *On Lee* in 1952 and *White* in 1971. *On Lee*, 343 U.S. 747; *White*, 401 U.S. 745.

82. *See On Lee*, 343 U.S. at 754 (discussing how Chin Poy and the Bureau of Narcotics used a transmitter and receiver to listen to On Lee's conversations);

B. A FORMER USER OF SOCIAL MEDIA CLAIMING FOURTH AMENDMENT PRIVACY AGAINST GOVERNMENT EXPLOITATION OF HER CONTACTS COULD RESURRECT "TARGET" STANDING AS PARTICULARLY APT FOR PREDICTIVE SURVEILLANCE

Persons wishing to contest predictive surveillance will have to contend with the Court's Fourth Amendment precedent regarding "standing."[83] Standing is the doctrine that states, "a person must have a cognizable Fourth Amendment interest in the place searched before seeking relief for an unconstitutional search."[84] At first blush, the Court's "standing" stance would undermine any claim of Fourth Amendment protection against predictive surveillance. In the seminal standing case, *Rakas v. Illinois*, the Court unequivocally ruled that the "capacity to claim the protection of the Fourth Amendment" depended on "whether the person who claims the protection of the Amendment has a legitimate expectation of privacy in the invaded place."[85] Arguing that one has a reasonable expectation of privacy in posts on social media seems doomed at the outset. However, as with many matters, the devil is in the details.

In *Rakas*, the defendants were passengers in an automobile in which police found "a box of rifle shells in the glove compartment, which had been locked, and a sawed-off rifle under the front passenger seat."[86] Even though the defendants conceded they did not own the car, rifle, or shells, they moved to suppress this evidence as recovered in violation of the Fourth Amendment.[87] The prosecutor responded that the defendants lacked standing to complain about a Fourth Amendment violation.[88] Noting that each application of the exclusionary rule blocked relevant evidence from court and therefore exacted a "substantial social cost," *Rakas* deemed Fourth Amendment

---

White, 401 U.S. at 746–47 (describing how Jackson used a radio transmitter so the police could listen to White's conversations).

83. *See generally* Rakas v. Illinois, 439 U.S. 128 (1979) (holding that Fourth Amendment rights cannot be vicariously asserted); Byrd v. United States, 138 S. Ct. 1518, 1530 (2018) (differentiating Fourth Amendment "standing" from Article III standing).

84. *Byrd*, 138 S. Ct. at 1530.

85. *Rakas*, 439 U.S. at 143.

86. *Id*. at 130.

87. *See id*. (outlining the defendant's arguments in favor of a motion to suppress).

88. *See id*. at 131 (outlining the prosecutor's response to defendant's motion to suppress).

rights as "personal rights" which could "not be vicariously asserted."[89] Therefore, vindication of Fourth Amendment rights was left to "defendants whose Fourth Amendment rights have been violated."[90]

Determining the precise identity of those suffering a Fourth Amendment violation caused the Court to question "whether it serves any useful analytical purpose" to consider standing as a concept "distinct from the merits of a defendant's Fourth Amendment claim."[91] In answer, *Rakas* ruled that standing, rather than being some "theoretically separate" inquiry, was simply the substantive Fourth Amendment question of "whether the challenged search or seizure violated the Fourth Amendment rights of a criminal defendant who seeks to exclude the evidence obtained during it."[92] Thus, when a person is contesting a search, the proper "standing" analysis applies *Katz*'s test: "whether the person who claims the protection of the [Fourth] Amendment has a legitimate expectation of privacy in the invaded place."[93] Since the defendants in *Rakas* "made no showing that they had any legitimate expectation of privacy in the glove compartment or area under the seat of the car in which they were merely passengers," their Fourth Amendment claims failed.[94]

In using *Katz* to assess standing, *Rakas* explicitly rejected a "target" test offered by the defendants.[95] Target standing would enable "any criminal defendant at whom a search was 'directed'" to contest the legality of the search because she was the "victim" of the police intrusion.[96] *Rakas* found target standing

89. *Id*. at 133–34, 137.

90. *Id*. at 134.

91. *Id*. at 138.

92. *Id*. at 140; *see also id.* at 139 (declaring that standing should instead be "more properly subsumed under substantive Fourth Amendment doctrine"). *Cf.* Byrd v. United States, 138 S. Ct. 1518, 1530 (2018) (softening the court's prior rejection of "standing" as a doctrine separate from the substantive Fourth Amendment inquiry and noting that *Rakas* urged that "standing" should not be viewed as "distinct" from the Fourth Amendment "merits" of a case); *Byrd*, 138 S. Ct. at 1530 (conceding that, "[t]he concept of standing in Fourth Amendment cases can be a useful shorthand for capturing the idea that a person must have a cognizable Fourth Amendment interest in the place searched before seeking relief for an unconstitutional search . . . .").

93. Rakas v. Illinois, 439 U.S. 128, 143 (1979).

94. *Id*. at 148.

95. *Id*. at 132–134.

96. *Id*. at 132.

problematic because it would disregard the personal nature of Fourth Amendment rights by allowing "a defendant to assert that a violation of the Fourth Amendment rights of a third party" supported suppression of evidence.[97]

There is perhaps one context in which *Rakas*'s concerns about target standing would not exist—predictive surveillance. Target standing's failure in enabling a person to assert someone else's Fourth Amendment rights to exclude evidence would not occur with predictive surveillance.[98] Were police to view the online posts of a person's contacts in order to predict that user's future conduct, the officers would not be violating the reasonable expectations of privacy of the contacts because no privacy expectations would exist in such public behavior.[99] The "targeted" user therefore would not be relying on the "search" of her contacts as third parties. Instead, the user would be claiming that law enforcement was gathering information about her own future conduct, even in circumstances where she had opted out of any social media entirely. Unlike prior defendants that have attempted to employ target standing, the only Fourth Amendment right a social media user subjected to predictive surveillance would be vindicating would be her own.

Target standing in predictive search cases would not only avoid the concerns raised in *Rakas*, but also provide the simplest theory to directly address the "programmatic purpose" behind law enforcement's predictive policing.[100] While *Whren v. United States* refused to consider an officer's subjective motivations relevant to a Fourth Amendment inquiry,[101] later decisions have examined subjective intent in the context of an agency's "programmatic purpose" in the "general scheme" of its institutional behavior.[102] In *City of Indianapolis v. Edmond*, the

---

97. *Id*. at 133.

98. *Id.* at 132–134.

99. *Id*. at 148. *See also* Brian Mund, *Social Media Searches and the Reasonable Expectation of Privacy*, 19 YALE J. L. & TECH. 238, 241–247 (2017) (arguing there is no reasonable expectation of privacy in social media posts because of the third-party doctrine and voluntary sharing).

100. *See* City of Indianapolis v. Edmond, 531 U.S. 32, 45–46 (2000) (noting that absent individualized suspicion, courts would look into programmatic purposes to determine the validity of Fourth Amendment intrusions).

101. The *Whren* Court noted, "[W]e have been unwilling to entertain Fourth Amendment challenges based on the actual motivations of individual officers." Whren v. United States, 517 U.S. 806, 813 (1996).

102. *Edmond*, 531 U.S. at 45–46.

Court found that a drug checkpoint program, operated without "reasonable suspicion or probable cause,"[103] violated the Fourth Amendment.[104] This was in spite of the fact that the Court had upheld suspicionless checkpoint programs in the past.[105] The fatal flaw in Indianapolis' checkpoint program was its "programmatic purpose," which was "the discovery and interdiction of illegal narcotics."[106] Since the city's aim was "to uncover evidence of ordinary criminal wrongdoing," performing these checkpoint stops without any Fourth Amendment individualized suspicion violated the Fourth Amendment.[107] If a law enforcement agency collects information on a user's contacts in order to predict that user's future behavior, it would be fair to say that the programmatic purpose of this intrusion "targets" the individual user rather than the contacts. This characterization is the most apt and clear description of police actions in predictive surveillance and therefore the most likely to inform the Fourth Amendment inquiry.

Target standing, when applied to predictive surveillance, would also effectively answer the two issues *Rakas* mandated that standing address: "first, whether the proponent of a particular legal right has alleged an 'injury in fact,' and, second, 'whether the proponent is asserting his own legal rights and interests rather than basing his claim for relief upon the rights of third parties.'"[108] As to *Rakas*' first inquiry, with predictive surveillance, the person who genuinely suffers an "injury in fact" is the target of the mathematical algorithms anticipating her behavior, not the users still posting messages online.[109] The user who has retreated from all social media suffers direct injury from predictive surveillance because she is still being pursued by police, regardless of her every effort to regain privacy. As to *Rakas*' second question, the victim of predictive surveillance rightly identifies the right implicated as her "own" because it is her private future that law enforcement is probing. Predictive

---

103. *Id*. at 35.

104. *Id*. at 48.

105. *See id*. at 34 (noting that the Supreme Court had held that "brief, suspicionless seizures at highway checkpoints for the purposes of combating drunk driving and intercepting illegal immigrants were constitutional").

106. *Id*.

107. *Id*. at 42.

108. Rakas v. Illinois, 439 U.S. 128, 139 (1979).

109. *Id*.

surveillance's fulfillment of *Rakas*'s own two criteria for answering the key questions for standing provides still further evidence for employing target standing in this unique context.

C. A REINTERPRETATION OF COURT PRECEDENT REGARDING A HOMEOWNER'S RIGHT TO PRIVACY, WHEN VIEWED WITH COURT RULINGS ON COLLECTION OF DIGITAL INFORMATION, COULD PROVIDE THE STRONGEST ARGUMENT FOR FOURTH AMENDMENT PROTECTION AGAINST PREDICTIVE SURVEILLANCE OF SOCIAL MEDIA

Any law enforcement agency using predictive surveillance would likely argue that, rather than intruding directly on the communications of the targeted individual, the government is merely collecting the current messages of each person who had previously communicated with the target.[110] As noted in the last section, the Court currently has little patience for those complaining about government intrusions on persons other than themselves.[111] Another potential path to Fourth Amendment protection could be established by considering three cases spanning half a century: *Alderman v. United States*,[112] *Riley v. California*,[113] and *Carpenter v. United States*.[114]

In *Alderman*, the Court protected an individual against government intrusion on communications even though the person himself was not a participant in those conversations.[115] After appellate courts affirmed the convictions for "conspiring to

---

110. *See* Rachel Levinson-Waldman, *Government Access to and Manipulation of Social Media: Legal and Policy Changes*, 61 HOWARD L. J. 523, 547 (2018) (discussing the case of *United States v. Meregildo* in which the court held police using a target's online friends to survey communications was not violation of the Fourth Amendment). *See also* Christopher Raleigh Bousquet, *Why Police Should Monitor Social Media to Prevent Crime*, WIRED (Apr. 20, 2018), https://www.wired.com/story/why-police-should-monitor-social-media-to-prevent-crime/ (arguing for increased police use of social media monitoring to predict crime and discussing the legal ramifications of doing so).

111. *See Rakas*, 439 U.S. at 132–134 (rejecting "target" standing which would allow someone to assert another's Fourth amendment rights).

112. Alderman v. United States, 394 U.S. 165 (1969).

113. Riley v. California, 573 U.S. 373 (2014).

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

115. *See Alderman*, 394 U.S. at 176 (holding that defendant was entitled to Fourth Amendment protections "if the United States unlawfully overheard conversations of a petitioner himself or conversations occurring on his premises, whether or not he was present or participated in those conversations").

transmit murderous threats in interstate commerce,"[116] the Court learned that the United States, potentially in violation of the Fourth Amendment, "had engaged in electronic surveillance"[117] of Alderisio's business premises in Chicago.[118] *Alderman* framed the issues as follows:

> What standards are to be applied in determining whether each petitioner has standing to object to the use against him of the information obtained from the electronic surveillance of petitioner Alderisio's place of business? More specifically, does petitioner Alderisio have standing to object to the use of any or all information obtained from such electronic surveillance whether or not he was present on the premises or party to a particular overheard conversation?[119]

The Court therefore considered whether a person has standing to contest government intrusions into conversations in which he is not a party. *Alderman* reaffirmed "the general rule that Fourth Amendment rights are personal rights"[120] which could "not be vicariously asserted."[121] The Court further reiterated, "suppression of the product of a Fourth Amendment violation can be successfully urged only by those whose rights were violated by the search itself, not by those who are aggrieved solely by the introduction of damaging evidence."[122]

After explicitly restating the personal nature of Fourth Amendment rights, *Alderman* declared that a violation would occur "if the United States unlawfully overheard conversations of a petitioner himself or conversations occurring on his premises, *whether or not he was present or participated in those conversations*."[123] The Court defended its ruling from dissenting Justices Harlan and Stewart, who objected "to our protecting the homeowner against the use of third-party conversations overheard on his premises."[124] The Court rejected the dissent's

---

116. *Id.* at 167.

117. *Id*.

118. *See id.* ("[P]etitioners alleged they had recently discovered that Alderisio's place of business in Chicago had been the subject of electronic surveillance by the Government."). *See also* United States v. Alderisio, 424 F.2d 20 at 21 n.2 (specifying that the government electronically monitored "the Gaylur Mercantile Company and the First National Mortgage Company").

119. *Alderman* 394 U.S. at n.2.

120. *Id*. at 174.

121. *Id.*

122. *Id*. at 171–72.

123. *Id*. at 176 (emphasis added).

124. *Id*.

position that "unless the conversational privacy of the homeowner himself is invaded, there is no basis in the Fourth Amendment for excluding third-party conversations overheard on his premises."[125] *Alderman* noted that if the government had illegally seized "tangible property belonging to third parties—even a transcript of a third-party conversation"[126] the homeowner would be able to contest the search simply because the evidence was the fruit of "an unauthorized search of his house, which is itself expressly protected by the Fourth Amendment."[127] The Court warned that the dissent would allow officers to enter a "house without consent and without a warrant, install a listening device, and use any overheard third-party conversations against the owner in a criminal case, in spite of the obvious violation of his Fourth Amendment right to be secure in his own dwelling."[128] *Alderman* rejected this approach, noting,

> The rights of the owner of the premises are as clearly invaded when the police enter and install a listening device in his house as they are when the entry is made to undertake a warrantless search for tangible property; and the prosecution as surely employs the fruits of an illegal search of the home when it offers overheard third-party conversations as it does when it introduces tangible evidence belonging not to the homeowner, but to others.[129]

Therefore, *Alderman* explicitly established that, in certain circumstances, the Fourth Amendment protected "third party conversations" even if the persons seeking privacy were not themselves involved in the overheard conversations.[130] The rationale supporting the protection, however, was based on the privacy rights of the homeowner.[131] *Kyllo v. United States*, a case involving government use of technology to intrude into a house, noted the special status of the home in Fourth Amendment jurisprudence.[132] *Kyllo* noted that, when it came to privacy, the

---

125. *Id*.
126. *Id*.
127. *Id*. at 177.
128. *Id*. at 178.
129. *Id*. at 179–80 (emphasis added).
130. *See id*. at 180 ("[C]onversations as well as property are excludable from the criminal trial when they are found to be the fruits of an illegal invasion of the home.").
131. *See id*. at 179 ("We adhere to the established view in this Court that the right to be secure in one's house against unauthorized intrusion is not limited to protection against a policeman viewing or seizing tangible property . . . .").
132. *See* Kyllo v. United States, 533 U.S. 27, 31 (2001) ("'At the very core' of the Fourth Amendment 'stands the right of a man to retreat into his own home

"Fourth Amendment draws 'a firm line at the entrance to the house.'"[133] This was because "[i]n the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes."[134]

While persons subject to predictive surveillance of their Twitter contacts may send some of their tweets from home, they cannot rely on the privacy of their premises as did Alderisio in the *Alderman* case. Such Twitter users send their messages to the Internet, a domain outside of the physical home. The Court, however, has recently determined, in *Riley v. California*, that some information in the digital realm has a privacy interest comparable to that in the home.[135] *Riley* involved officers looking through cellphones obtained from two arrestees.[136] In *Riley*'s first case, police, after arresting David Riley for "possession of concealed and loaded firearms,"[137] located photographs on his phone showing Riley standing in front of a car suspected of being connected with an earlier shooting.[138] In the second case, police caught Brima Wurie apparently selling drugs.[139] A search of Wurie's "flip phone" ultimately led to police seizing drugs and guns from an address found on the phone.[140] When the police in both cases justified their collection of cellphone evidence as obtained by search incident to arrest, the Court refused to extend this search warrant exception to digital information.[141]

---

and there be free from unreasonable governmental intrusion.'") (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)). *Kyllo* involved government "use of a thermal-imaging device aimed at a private home from a public street to detect relative amounts of heat within." *Id*. at 29.

133. *Id*. at 40 (quoting Payton v. New York, 445 U.S. 573, 590 (1980)).

134. *Id*. at 37.

135. *See* Riley v. California, 573 U.S. 373, 396–97 (2014) ("[A] cell phone search would typically expose to the government far more than the most exhaustive search of a house . . . .").

136. *Id*. at 378–79, 380.

137. *Id*. at 378.

138. *See id*. at 379 (explaining that while "there was 'a lot of stuff' on the phone, particular files . . . 'caught [the detective's] eye . . . '").

139. *See id*. at 380 ("[A] police officer performing routine surveillance observed respondent Brima Wurie make an apparent drug sale from a car.").

140. *See id*. at 381 (specifying that police "found and seized 215 grams of crack cocaine, marijuana, drug paraphernalia, a firearm and ammunition, and cash").

141. *See id*. at 386 (holding that the general exception to the warrant requirement for searches incident to arrest did not extend to data on cell phones).

In assessing searches of smartphones incident to arrest, *Riley* drew a distinct line between "physical objects," such as a package of cigarettes,[142] and the "digital content on cell phones."[143] A search of a cellphone gave the government access to such "vast quantities of personal information" that it bore "little resemblance" to traditional searches of physical items.[144] *Riley* declared that equating searches of physical objects and cellphones "is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together."[145] The Court therefore put digital information stored on devices such as smartphones in an entirely separate "category" with protections "far beyond" such physical items as "a cigarette pack, a wallet, or a purse."[146] In doing so, *Riley* equated the privacy interest in a smartphone with that in the home:

> [A] cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.[147]

The digital information stored in a smartphone was therefore of such a great capacity and sensitivity that the Court found it rivaled or exceeded the privacy interests in the home—the Fourth Amendment's "core."[148]

The digital information on a cellphone shares many similarities with the digital information found in social media accounts online. *Riley* noted that smartphones "could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or

---

142. *Id.* at 383–386.
143. *Id.* at 386.
144. *Id.*
145. *Id.* at 393.
146. *Id.*
147. *Id.* at 396–97.
148. *See* Kyllo v. United States, 533 U.S. 27, 31 (2001). The court has asserted, "'At the very core' of the Fourth Amendment 'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'" *Id.* (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)). Further, the Justices have recognized that a search of the home implicates one of the "core areas of privacy." California v. Carney, 471 U.S. 386, 405 (1985) (Stevens, J., dissenting) (quoting United States v. Chadwick, 433 U.S. 1, 7 (1977)).

newspapers."[149] Social media fulfills many of these same functions. Facebook, by allowing the sharing of photos and videos, fulfills the functions of cameras, videos players, and tape recorders. Instead of a Rolodex and a calendar, Facebook has a "friends" list and an "events" feature. Facebook's timeline and Instagram's profile and stories are analogous to diaries. Finally, these services have newsfeeds, which users share and over which they debate. Indeed, the main difference between social media and the collection of devices *Riley* listed in smartphones is that social media combines and amplifies these various functions to create a more immersive, perhaps even addictive, experience.[150] Using these services therefore might cause us to expose more of ourselves than we ever would in a mere calendar or Rolodex.

Further, *Riley* declared that cellphones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[151] To say that social media is pervasive would be an understatement; Twitter has recently reported having "126 million daily active users" while Facebook has logged in at "1.2 billion daily users."[152] For perspective, the number of Twitter users exceeds the population of Mexico in 2018 (estimated at over 125 million for July 2020)[153] and the number of Facebook users is well over three times the population of the United States in 2018 (estimated at over 327 million for July 1, 2019).[154] Further, much of the very pervasiveness and

149. Riley v. California, 573 U.S. 373, 393 (2014).

150. *See Social Media Addiction*, ADDICTION CTR., https://www.addictioncenter.com/drugs/social-media-addiction/ (last visited Feb. 16, 2020) (explaining a percentage of users become addicted to social media).

151. *Riley*, 573 U.S. at 385. *Riley* also wondered at the "pervasiveness that characterizes cell phones," noting that the person not carrying a cellphone was the "exception" in our society. *Id.* at 395.

152. Hamza Shaban, *Twitter Reveals Its Daily Active User Numbers for the First Time*, WASH. POST (Feb. 7, 2019, 10:43 AM), https://www.washingtonpost.com/technology/2019/02/07/twitter-reveals-its-daily-active-user-numbers-first-time.

153. Cent. Intelligence Agency, *Mexico*, THE WORLD FACTBOOK (Feb. 5, 2020), https://www.cia.gov/library/publications/the-world-factbook/geos/mx.html.

154. U.S. Census Bureau, *QuickFacts: United States*, CENSUS.GOV, https://www.census.gov/quickfacts/fact/table/US/PST045218 (last visited Feb. 20, 2020).

insistency *Riley* noted about smartphones came from the fact that they performed a function much like modern social media.[155] Social media is so firmly rooted in our daily lives that seventy percent of respondents in a *Wall Street Journal/NBC News* survey reported that they "check in daily."[156] Therefore, if *Riley* worried that an officer's opening of a cellphone would permit deep and broad access to many aspects of a person's life, no less a concern is presented by government entry into an individual's online activity.

Finally, *Riley* noted that cellphone owners "keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate."[157] The same could be said of the digital record left by social media users who likewise share the mundane, such as a plate of food at a restaurant, and the intimate, whether it be relationship statuses or health updates. When *Riley* worried that the "sum of an individual's private life" on cellphones could "be reconstructed through a thousand photographs labeled with dates, locations, and descriptions," the Court could have been discussing the timeline of Facebook or the profile and stories of Instagram.[158] This, in a sense, is the very purpose of Facebook—to construct a version of one's life. Finally, *Riley* was troubled by the fact that "the data on a phone can date back to the purchase of the phone, or even earlier."[159] Similarly, the data in social media accounts, stored in the Cloud, continue to exist over the years from one's first post.[160] Moreover, the predictive surveillance revealed by Bagrow and his peers presents a danger not even contemplated by *Riley*—that the

---

155. *See* Riley v. California, 573 U.S. 373, 393 (2014) ("The term 'cell phone' is itself misleading shorthand; many of these devices . . . .could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.").

156. John D. McKinnon & Danny Dougherty, *Americans Hate Social Media But Can't Give It Up, WSJ/NBC News Poll Finds*, WALL ST. J. (Apr. 5, 2019, 5:30 PM), https://www.wsj.com/articles/americans-agree-social-media-is-divisive-but-we-keep-using-it-11554456600.

157. *Riley*, 573 U.S. at 395.

158. *Id.* at 394.

159. *Id.*

160. *See How Long Does Your Data Remain on the Internet*, VTNV SOL.'S LTD. (Sept. 26, 2018), https://www.le-vpn.com/long-data-remain-internet/ (explaining that data uploaded to social media "may be searchable forever" and that data storage in the Cloud means that "in most cases data you upload, access, store, and use will at some point get used by, stored and saved on some third party server").

government could conceivably obtain information not only about a person's past behavior, but her future.[161]

The argument for social media privacy from predictive surveillance is strengthened when *Alderman* and *Riley* are combined with *Carpenter v. United States*, a case involving government collection of the location information of cellphones.[162] As *Carpenter* explained, today's smartphones "continuously scan" their environment to gain "the best signal, which generally comes from the closest cell site."[163] Every time a "phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI)."[164] This process occurs automatically, regardless of whether a person is using the phone or not.[165] In 2011, police in Detroit exploited this technology to connect Timothy Carpenter to a series of robberies.[166] Armed with a federal court order directing MetroPCS and Sprint to provide CSLI for Carpenter's phone, the government gathered "12,898 location points cataloging Carpenter's movements—an average of 101 data points per day" for up to 152 days.[167] Prosecutors used this evidence to place Carpenter's phone "near four of the charged robberies."[168] Since this evidence demonstrated that Carpenter was "right where the . . . robbery was at the exact time of the robbery," it "clinched the case."[169]

The *Carpenter* Court was clearly uncomfortable with the power of CSLI, warning, "technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes."[170] The Court worried about people being "at the mercy of advancing technology"[171] and of a "too permeating police surveillance."[172] *Carpenter* therefore aimed to preserve "that degree of privacy against government that existed

---

161. *See* Hutson, *supra* note 3 (explaining that computer scientists can predict the content of future postings).
162. Carpenter v. United States, 138 S. Ct. 2206 (2018).
163. *Id*. at 2211.
164. *Id*.
165. *Id*.
166. *Id*. at 2212.
167. *Id*.
168. *Id*. at 2213.
169. *Id*.
170. *Id*. at 2214.
171. *Id.*
172. *Id*. (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

when the Fourth Amendment was adopted."[173] The Court reiterated that the Fourth Amendment was meant "to secure 'the privacies of life' against 'arbitrary power'"[174] and recalled that the founders crafted this right to protect against British officers committing "unrestrained" searches.[175]

Carpenter was particularly alarmed by the intrusiveness and pervasiveness of CSLI technology. Collection of CSLI enabled the government to easily create an "exhaustive chronicle of location information" detailing where a person was,[176] on average, every quarter hour for months or years at a time.[177] *Carpenter* emphasized that the "cell phone location information is detailed, encyclopedic, and effortlessly compiled."[178] The Court therefore ruled, "when the Government accessed CSLI from the wireless carriers, it invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements."[179] *Carpenter* held, "[t]he Government's acquisition of the cell-site records was a search within the meaning of the Fourth Amendment."[180]

The Court found CSLI was protected by the Fourth Amendment despite the public nature of the information. A smartphone user "continuously reveals his location to his wireless carrier" and therefore shares the whereabouts of his phone with a third party, the cell service provider.[181] *Carpenter* acknowledged that earlier precedent, starting with *United States v. Miller*,[182] had created the "third-party doctrine" which refused to find a reasonable expectation of privacy in information shared with another person or entity.[183] Specifically, the Court conceded, "[w]e have previously held that 'a person has no legitimate expectation of privacy in information

---

173. *Id*. (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)).
174. *Id*.
175. *Id*. at 2213.
176. *Id*. at 2219.
177. The CSLI information of *Carpenter* averaged "101 data points per day" for more than 100 days with one phone service provider. *Id*. at 2212. The Court noted that "wireless carriers" maintained records "for up to five years." *Id*. at 2218.
178. *Id*. at 2216.
179. *Id*. at 2219.
180. *Id*. at 2220.
181. *Id*. at 2216.
182. United States v. Miller, 425 U.S. 435 (1976).
183. *Carpenter* 138 S. Ct. at 2216.

he voluntarily turns over to third parties.'"[184] Therefore, the defendant in *Miller* lacked any reasonable expectation of privacy, and therefore a Fourth Amendment claim, in the "canceled checks, deposit slips, and monthly statements" the government sought by subpoena because he had shared such information with his bank, a third party.[185] Similarly, in *Smith v. Maryland*,[186] when the government used a "pen register" to collect the numbers a caller dialed in placing a phone call, the Court found the caller lacked a reasonable privacy expectation in these dialed numbers.[187] The phone caller had squandered his privacy by voluntarily conveying this information "to a telephone company."[188]

Carpenter found *Miller* and *Smith* did not limit a smartphone user's privacy in CSLI.[189] Even though a smartphone user's continuous exposure of "his location to his wireless carrier" implicated *Miller* and *Smith*'s "third-party principle," it was not clear to the Court that this doctrine's "logic extend[ed] to the qualitatively different category of cell-site records."[190] Quite simply, CSLI's "detailed and comprehensive record" of a phone user's movements[191] dwarfed the information obtained by the "limited capabilities" of the old-fashioned pen register.[192] *Carpenter* concluded: "Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection."[193]

Due to the invasiveness of predictive surveillance, the Court might someday follow *Carpenter*'s lead, finding Fourth Amendment protection against this intrusion despite the fact that social media users have shared information with others. With both CSLI and platforms such as Facebook and Twitter, technology has crafted "an intimate window into a person's life," revealing "familial, political, professional, religious, and sexual

184. *Id*. (citing Smith v. Maryland, 442 U.S. 735, 743–44 (1979)).
185. *Id*.
186. Smith v. Maryland, 442 U.S. 735 (1979).
187. *Carpenter*, 138 S. Ct. at 2216.
188. *Id*.
189. *Id*.
190. *Id*. at 2216–17.
191. *Id*. at 2217.
192. *Id*. at 2216.
193. *Id*. at 2217.

associations," and therefore the "privacies of life."[194] While CSLI provided "an all-encompassing record of the holder's whereabouts," predictive surveillance arguably intrudes even further by building an all-encompassing record of a person's online statements, and therefore, her thoughts.[195] While *Carpenter* fretted about wireless carriers' retention of a person's movements "every moment of every day for five years,"[196] Twitter and other social media platforms hold records of personal behavior beyond a mere five years.[197] Facebook even has a legacy option for deceased Facebook users, making the use of an account last beyond a lifetime.[198] *Carpenter* was alarmed that CSLI gave the government "easy, cheap, and efficient" access to a "deep repository" of historical information with "just a click of a button."[199] These same concerns could exist with predictive surveillance's exploitation of social media platforms.

Of particular interest for predictive surveillance issues are *Carpenter*'s concerns regarding the time-traveling nature of CSLI. The Court recognized that CSLI surveillance had a "retrospective quality" which gave law enforcement access "to a category of information otherwise unknowable."[200] CSLI enabled the government to "travel back in time to retrace a person's whereabouts."[201] CSLI's ability to "chronicle a person's past movements" forced the Court to "confront" a "new phenomenon," a kind of surveillance the government previously "simply could not" perform.[202] CSLI time-travel is based on the fact that

---

194. *Id*. (quoting United States v. Jones, 565 U.S. 400, 415 (1948) (Sotomayor, J., concurring)).

195. *Id*.

196. *Id*. at 2218.

197. Twitter had its tenth "birthday" in 2016. *We Look Back at Famous First Tweets As Twitter Turns 10*, BBC NEWSBEAT (Mar. 20, 2016), http://www.bbc.co.uk/newsbeat/article/35857514/we-look-back-at-famous-first-tweets-as-twitter-turns-10. Longtime Twitter users are discussed in Charles Arthur, *How Twitter Was Born: The First 140 Users*, THE GUARDIAN (Jan. 11, 2010), https://www.theguardian.com/technology/blog/2010/jan/11/twitter-first-140-users-history.

198. Facebook has made a "memorialized account" option for those who have passed away. *Memorialized Accounts*, FACEBOOK, https://www.facebook.com/help/1506822589577997 (last visited Feb. 10, 2020). Facebook users can appoint a "legacy contact" to look after one's account. *Id*.

199. *Carpenter*, 138 S. Ct. at 2217–18.

200. *Id*. at 2218.

201. *Id*.

202. *Id*. at 2216–2217 (quotations omitted).

wireless providers continually log location information "for all of the 400 million devices in the United States."[203] Police therefore need not "know in advance whether they want to follow a particular individual or when."[204] Having the luxury of knowing that information is being continuously collected, law enforcement can go back in time whenever it wishes to tail any individual for "every moment of every day" for a matter of years.[205] With predictive surveillance, social media users would be subject to the same kind of "tireless and absolute surveillance."[206] Predictive surveillance, however, could be even more intrusive than CSLI because this new technology delves into not only a person's past but also her future. The Court could rightly ask how a person could reasonably anticipate the exposure of her future interactions with others, particularly the government, when she herself cannot even divine this "otherwise unknowable" frontier.[207]

Another reason that *Carpenter* refused to apply *Miller* and *Smith*'s third-party doctrine to CSLI involved voluntariness. When Miller did his banking, he chose to share his checks and deposit slips with the bank.[208] When Smith dialed his phone, he likewise meant to share his phone number with the phone company.[209] Carpenter, when passively possessing his smartphone, did not similarly commit "voluntary exposure" because cellphones have become "such a pervasive and insistent part of daily life" that carrying one is indispensable to participation in modern society."[210] Unless one committed the extreme step of "disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data."[211] *Carpenter* therefore concluded, "in no meaningful sense does the user voluntarily 'assume the risk' of turning over a

---

203. *Id*. at 2218.

204. *Id*.

205. *Id.*

206. *Id*.

207. *See id.* ("Moreover, the retrospective quality of the data here gives police access to a category of information otherwise unknowable.").

208. United States v. Miller, 425 U.S. 435, 442 (1976) (finding that Miller "voluntarily conveyed" his banking information).

209. Smith v. Maryland, 442 U.S. 735, 744 (1979) (finding that Smith "voluntarily conveyed numerical information").

210. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (citations omitted)

211. *Id*.

comprehensive dossier of his physical movements."[212] Many would argue that social media—in keeping users in touch with friends and loved ones, alerting them to the latest news, offering the needed escape of a humorous video, and providing birthday reminders—has become an equally integral part of society that people are loathe to give up. *Carpenter* also distinguished between using a smartphone and voluntarily banking or dialing on a landline by noting that CSLI information is collected "without any affirmative act on the part of the user beyond powering up."[213] The Court noted that "[v]irtually any activity on the phone," including social media updates, generates CSLI.[214] Predictive surveillance exploits this same aspect of connectivity; even if a user leaves social media and takes no further volitional action, the government can predict future behavior by scrutinizing followers—actions of others beyond a former user's control. With CSLI, *Carpenter* warned, "[a]part from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data."[215] Former social media users trying to escape the reach of predictive surveillance lack even this dire option.

In holding that government CSLI collection was a search, *Carpenter* revitalized Fourth Amendment protection in public places.[216] The Court declared, "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere" because what a person "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[217] Such language could bode well for social media users who fear an intrusion from predictive surveillance. As *Carpenter* warned, "the Court is obligated—as '[s]ubtler and more far-reaching means of invading privacy have become available to the Government'—to ensure that the 'progress of science' does not erode Fourth Amendment protections."[218]

---

212. *Id*. (quotations and citations omitted).

213. *Id*.

214. *See id*. (listing other activities including "incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates").

215. *Id*.

216. *See id*. at 2218

217. *Id*. (quoting Katz v. United States, 389 U.S. 347, 351–52 (1967)).

218. *Id*. at 2223 (quoting Olmstead v. United States, 277 U.S. 438, 473–74 (1928)).

V. CONCLUSION

In his advanced years, Cicero, the great Roman orator and statesman, wrote in his *Treatise on Friendship* about a friend, "What can be more delightful than to have some one to whom you can say everything with the same absolute confidence as to yourself?"[219] Cicero declared, "In the face of a true friend a man sees as it were a second self."[220] Cicero could not imagine that, with the advent of advanced mathematics scouring social media, his statement would take on even greater truth. In the near future, the government could, when scrutinizing a person's contacts on social media, create a second version of that original user. This statistical construct, from the target's friends and not reliant on any information from the targeted individual, could then predict the target's future conduct.[221]

Over half a century ago, government agents in *Silverman v. United States* penetrated a house with a "spike mike" to overhear conversations about illegal gambling.[222] *Silverman* found this intrusion to violate the Fourth Amendment because "[a]t the very core stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion."[223] The Court refused to allow the government to "secretly observe or listen" to what occurs in the home without the protection of a Fourth Amendment warrant.[224]

Social media, of course, resides not in a person's home but in the Cloud. *Riley* began to grapple with the reality that people now depend on the privacy of information in the digital realm much as they do with information in their homes.[225] If at the core of the Fourth Amendment, a person has the right to "retreat into

---

219. MARCUS TULLIUS CICERO, LETTERS OF MARCUS TULLIUS CICERO WITH HIS TREATISES ON FRIENDSHIP AND OLD AGE 15 (E. S. Shuckburg trans. 1909).

220. *Id*.

221. Such technology could potentially be so powerful that it falsifies the statement made by the famous science fiction writer, Philip K. Dick, in his short story, *The Minority Report*, "there can be no valid knowledge about the future." Philip K. Dick, "*The Minority Report*," *in* THE MINORITY REPORT AND OTHER CLASSIC STORIES BY PHILIP K. DICK 71, 99 (Citadel Press, Kensington Publishing Group, 1987).

222. Silverman v. United States, 365 U.S. 505, 506 (1961).

223. *Id*. at 511.

224. *Id*. at 511–12; *see also* Kyllo v. United States, 533 U.S. 27, 37 (2001) (reiterating that the area in a home is to be "held safe from prying government eyes").

225. Riley v. California, 573 U.S. 373, 396–97 (2014).

his own home,"[226] an individual should likewise have the equivalent right to "retreat" from social media.[227] If instead the Court in the future allows law enforcement to pursue a person by predicting her behavior from others' posts even after she has "retreated" from social media by deleting her account, then it has failed to guard against "the seismic shifts in digital technology."[228] The Court has already explored doctrines that could provide protection against predictive surveillance of a social media users' contacts: target standing, the right of homeowners in the privacy of any communications on their premises, and the recognition of the need for privacy in digital information. Ultimately, privacy in this realm will depend on whether the Court will value protecting us from the indiscretion of friends.

226. *Silverman*, 365 U.S. at 511.
227. *Riley*, 573 U.S. at 396–97.
228. Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).