




2022

Facebook, Crime Prevention, and the Scope of the Private Search Post-Carpenter

Connor M. Correll
University of Georgia School of Law

Follow this and additional works at: <https://digitalcommons.law.uga.edu/blr>

 Part of the [Computer Law Commons](#), [Criminal Procedure Commons](#), and the [Fourth Amendment Commons](#)

Recommended Citation

Correll, Connor M. (2022) "Facebook, Crime Prevention, and the Scope of the Private Search Post-Carpenter," *Georgia Law Review*. Vol. 56: No. 2, Article 6.
Available at: <https://digitalcommons.law.uga.edu/blr/vol56/iss2/6>

This Note is brought to you for free and open access by Digital Commons @ University of Georgia School of Law. It has been accepted for inclusion in Georgia Law Review by an authorized editor of Digital Commons @ University of Georgia School of Law. [Please share how you have benefited from this access](#) For more information, please contact tstriepe@uga.edu.

Facebook, Crime Prevention, and the Scope of the Private Search Post-Carpenter

Cover Page Footnote

J.D. Candidate, 2022, University of Georgia School of Law; B.S., 2018, Wingate University. The author thanks Professor Thomas E. Kadri for his advice regarding this Note and Cassidy Correll for her love and constant support.

FACEBOOK, CRIME PREVENTION, AND THE SCOPE OF THE PRIVATE SEARCH DOCTRINE POST-CARPENTER

*Connor M. Correll**

The Fourth Amendment of the U.S. Constitution protects people “against unreasonable searches and seizures.” The private search doctrine provides a notable exception to the Fourth Amendment, providing that the government may reconstruct a search previously performed by a private party without first obtaining a warrant. The U.S. Supreme Court developed the private search doctrine prior to the advent of the internet; however, modern technology has changed the way that individuals live. What was once done entirely in private is now done alongside ever-present third parties, such as cell phones and virtual assistants.

Facebook and other social media sites complicate Fourth Amendment jurisprudence even further. Facebook collects a vast amount of information from its users, which total over 300 million in the United States alone, in order to run its platform. While some of this information, such as content posted on a user’s timeline and lists of pages a user “likes,” is available to other Facebook users, other information, such as cookies, network and device information, and GPS location, is available only to Facebook.

What happens if Facebook voluntarily discloses user information to law enforcement, either to help solve a crime or to prevent possible commission of a crime, without law enforcement first seeking to legally obtain that information? Two recent U.S. Supreme Court cases, United States v. Jones and Carpenter v. United States, provide the Court with a pathway to protecting this information under the Fourth

* J.D. Candidate, 2022, University of Georgia School of Law; B.S., 2018, Wingate University. The author thanks Professor Thomas E. Kadri for his advice regarding this Note and Cassidy Correll for her love and constant support.

Amendment. In Jones, a “shadow-majority” of the Court concluded that individuals maintain a reasonable expectation of privacy in the aggregated sum of their public movements revealed by GPS monitoring and are therefore afforded Fourth Amendment protection. The Court in Carpenter cemented this reasoning by holding that individuals maintain a reasonable expectation of privacy in years of location information compiled by wireless carriers and that wireless carriers violate the Fourth Amendment when they provide that information to the government absent a warrant.

This Note argues that, based on the reasoning of Carpenter and Jones, individuals maintain a reasonable expectation of privacy in social media information that is not otherwise viewable by other users and that this information should therefore be afforded Fourth Amendment protection.

TABLE OF CONTENTS

I. INTRODUCTION.....	790
II. FACEBOOK’S COLLECTION OF USER DATA	793
III. BACKGROUND ON THE FOURTH AMENDMENT	797
A. DEFINING A “SEARCH” UNDER THE FOURTH AMENDMENT	797
B. THE PRIVATE SEARCH DOCTRINE	798
C. THE UNCERTAINTY OF THE STORED COMMUNICATIONS ACT	800
D. THE INFLUENCE OF TECHNOLOGY ON THE FOURTH AMENDMENT AND THE PRIVATE SEARCH DOCTRINE..	802
IV. EXCLUDING THE PRIVATE SEARCH DOCTRINE FROM FACEBOOK DATA	806
A. REASONABLE EXPECTATION OF PRIVACY IN FACEBOOK DATA	807
B. EXCLUDING THE PRIVATE SEARCH DOCTRINE FROM THE COLLECTION OF FACEBOOK DATA.....	810
C. DRAWING THE LINE: WHAT INFORMATION MAY LAW ENFORCEMENT REVIEW WITHOUT FIRST OBTAINING A WARRANT?.....	812
V. ANSWERING POTENTIAL CRITICISM	814
VI. CONCLUSION	817

I. INTRODUCTION

Since becoming available in 2004, Facebook has come to hold an important, almost indispensable place in the lives of millions of people in the United States.¹ Facebook has fundamentally changed the ways that we communicate: what used to be done by letter, email, or even face-to-face conversation is now often done by posting to a “friend’s” timeline or sending them a private message through Facebook Messenger.² Accompanying this communication revolution is a seismic shift in technology that has made it easier for Facebook to monitor its 302 million users in the United States.³ Facebook collects a vast amount of information from its users—ranging from posts, messages, and basic information provided when users create their accounts, to network and device information, cookie data, and recent activity—to provide a better experience across its platforms.⁴ While some of the information that Facebook collects is available to other users, such as content posted on timelines and lists of pages “liked” by users, many types of information are not available to other Facebook users.⁵ The information available to users includes content such as recently read articles, active sessions, and pages and user profiles recently viewed, among other forms of information.⁶

Facebook also provides some of the user information that it collects to law enforcement.⁷ Some policies are intended to protect

¹ See John Gramlich, *10 Facts About Americans and Facebook*, PEW RSCH. CTR. (June 1, 2021), <https://www.pewresearch.org/fact-tank/2021/06/01/facts-about-americans-and-facebook/> (explaining how prevalent Facebook use is in the United States).

² See Statista Rsch. Dep’t, *Most Popular Global Mobile Messaging Apps 2021*, STATISTA (Nov. 2, 2021), <https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps> (noting that there are 1.3 billion monthly active users on Facebook Messenger as of October 2021).

³ Statista Rsch. Dep’t, *United States: Number of Facebook Users 2017–2025*, STATISTA (Aug. 23, 2021), <https://www.statista.com/statistics/408971/number-of-us-facebook-users>.

⁴ See *Data Policy*, FACEBOOK, <https://www.facebook.com/about/privacy> (last visited Jan. 29, 2022) (describing the types of information that Facebook collects).

⁵ See *id.* (explaining that Facebook collects public information, such as communications with other users, as well as private information that others cannot see, such as device information, connections and network information, and usage information).

⁶ *What Categories of My Facebook Data Are Available to Me?*, FACEBOOK, <https://www.facebook.com/help/930396167085762> (last visited Jan. 29, 2022).

⁷ See *Information for Law Enforcement Authorities*, FACEBOOK,

those at risk of self-harm: Facebook’s current suicide prevention policy allows users to report posts that may indicate that a user is contemplating self-harm; trained members of Facebook’s Community Operations team then review these reported posts and can connect the users to mental health resources.⁸ In addition to receiving reports from users, Facebook uses artificial intelligence to provide help to those users who need it.⁹ When a Facebook team member or computer algorithm determines that an individual is at imminent risk of self-harm, Facebook contacts first responders and police to conduct a wellness check on that person.¹⁰ Other policies are linked to criminal behavior: while Facebook does not have such a robust reporting procedure for criminal behavior, the site does provide information to law enforcement to “help them respond to emergencies, including those that involve the immediate risk of harm, suicide prevention and the recovery of missing children.”¹¹ Facebook may also supply police “with information to help prevent or respond to fraud and other illegal activity, as well as violations of the Facebook Terms.”¹²

What happens if Facebook voluntarily discloses user information to law enforcement, either to help solve a crime or to prevent the possible commission of a crime, without law enforcement first seeking to legally obtain that information? While Facebook claims that it is attuned to privacy concerns,¹³ Facebook and other social

<https://www.facebook.com/safety/groups/law/guidelines/> (last visited Jan. 29, 2022) (detailing Facebook policies that relate to providing information to law enforcement).

⁸ See *Suicide Prevention*, FACEBOOK, <https://www.facebook.com/safety/wellbeing/suicideprevention> (last visited Jan. 29, 2022) (outlining Facebook’s suicide prevention policy).

⁹ See Catherine Card, *How Facebook AI Helps Suicide Prevention*, META (Sept. 10, 2018, 6:00 AM), <https://about.fb.com/news/2018/09/inside-feed-suicide-prevention-and-ai/> (“This [machine learning] tool uses signals to identify posts from people who might be at risk, such as phrases in posts and concerned comments from friends and family.”).

¹⁰ See *Suicide Prevention*, *supra* note 8 (explaining when Facebook contacts emergency services for mental health support); see also Card, *supra* note 9 (noting that Facebook contacted first responders to conduct over 1,000 wellness checks within the first year of implementing its machine learning suicide prevention tool).

¹¹ *Facebook and Law Enforcement*, FACEBOOK, <https://www.facebook.com/safety/groups/law> (last visited Jan. 27, 2022).

¹² *Id.*

¹³ See *id.* (stating that Facebook “take[s] the privacy of [user] information very seriously”). Despite Facebook’s assurances, it has a history of major user data leaks. For example, the

media giants are keenly aware of their ability to keep communities safe and advance social interests by providing law enforcement with certain user information.¹⁴ One need only look to the debate surrounding allegations of social media sites censoring conservative speech on their networks—in particular, over revoking Section 230 of the Communications Decency Act¹⁵ and former President Donald Trump’s ban from nearly all major social media platforms¹⁶—to see a recent example of technology giants wrestling with the idea of what their role in society should be.¹⁷ Thus, there is a need to

Cambridge Analytical scandal leading up to the 2016 United States presidential election involved a data firm improperly accessing the data of 87 million Facebook users. Cecilia Kang & Sheera Frenkel, *Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users*, N.Y. TIMES (Apr. 4, 2018), <https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html>. Despite Facebook’s claims that it implemented sweeping measures to curb potential data leaks, the social media company continued to fall victim to leaks. See Michael Nuñez, *Facebook Is Still Leaking Data More Than One Year After Cambridge Analytica*, FORBES (Nov. 5, 2019, 7:53 PM), <https://www.forbes.com/sites/mnunez/2019/11/05/facebook-is-still-leaking-data-more-than-one-year-after-cambridge-analytica/> (noting that 100 application developers accessed user data improperly in 2019).

¹⁴ See *Facebook and Law Enforcement*, *supra* note 11 (“We work with law enforcement to help people on Facebook stay safe.”); *Snapchat Safety Center*, SNAP INC., <https://snap.com/en-US/safety/safety-center> (last visited Jan. 29, 2022) (“Snap is deeply committed to the safety and wellbeing of our community, and our teams, products, policies, and partnerships apply safety by design principles to keep Snapchatters safe and informed.”); *Information for Law Enforcement*, SNAP INC., <https://snap.com/en-US/safety/safety-enforcement> (last visited Jan. 29, 2022) (explaining that Snapchat reviews allegations of “potential child exploitation content” and may report “such situations to the National Center for Missing and Exploited Children”).

¹⁵ 47 U.S.C. § 230. Section 230 prohibits treating internet service providers as publishers and shields such providers from civil liability for restricting access to certain material. *Id.* § 230(c).

¹⁶ See Alex Hern, *Opinion Divided over Trump’s Ban from Social Media*, GUARDIAN (Jan. 11, 2021, 1:17 PM), <https://www.theguardian.com/us-news/2021/jan/11/opinion-divided-over-trump-being-banned-from-social-media> (detailing the technology firms that banned Trump and the arguments for and against the firms’ decisions).

¹⁷ See, e.g., Tony Romm, Rachel Lerman, Cat Zakrzewski, Heather Kelly & Elizabeth Dvoskin, *Facebook, Google, Twitter CEOs Clash with Congress in Pre-Election Showdown*, WASH. POST (Oct. 28, 2020), <https://www.washingtonpost.com/technology/2020/10/28/twitter-facebook-google-senate-hearing-live-updates/> (summarizing the Senate Commerce Committee’s hearing with Twitter, Facebook, and Google executives regarding Section 230 and alleged censoring of conservative speech on social media). Commentators described a Senate hearing on these issues as leaving “Facebook, Google and Twitter facing conflicting pressures—from Democrats who say they should patrol their sites and services more

determine what information, if any, a social media company such as Facebook can disclose to law enforcement absent a warrant.

Based on reasoning from recent U.S. Supreme Court cases, this Note argues that individuals maintain a reasonable expectation of privacy in social media information not otherwise viewable by other users and that such information thus ought to be afforded Fourth Amendment protection. This Note starts by exploring Facebook's data collection policies and Fourth Amendment jurisprudence, specifically focusing on how the U.S. Supreme Court has dealt with technology developments. Next, this Note argues that there is a reasonable expectation of privacy in non-public social media information in two parts: First, this Note demonstrates that data collected by Facebook provides a wealth of information that can be used to gain insight into significant parts of an individual's life. Second, because Facebook is such an indispensable part of many users' lives, and because Facebook collects information even when an individual is not using Facebook at a given time, this Note explains that individuals cannot avoid having their information collected and potentially distributed, short of deleting their accounts. This Note then proposes a bright-line rule for when law enforcement should need a warrant to view this information and responds to potential criticism of this approach.

II. FACEBOOK'S COLLECTION OF USER DATA

Facebook collects individual information to provide a better experience for its users across its platforms, including Facebook, Messenger, Instagram, WhatsApp, and other products.¹⁸ Facebook collects user information, such as content that is shared with other users and basic information that individuals provide when they sign

aggressively and Republicans who felt the companies should have a more hands-off role with most political speech." They also noted that "[t]he mixed signals threatened to add new complications to the tech giants' already controversial work to protect the world's most popular digital communications channels from abuse." *Id.*

¹⁸ See *Data Policy*, *supra* note 4 (describing what types of information Meta, the parent company of Facebook, collects); Sam Shead, *Facebook Owns the Four Most Downloaded Apps of the Decade*, BBC (Dec. 18, 2019), <https://www.bbc.com/news/technology-50838013> (noting that Facebook, now called Meta, owns the four most downloaded apps of the 2010s: Facebook, Messenger, WhatsApp, and Instagram).

up for an account.¹⁹ This basic information includes data such as locations where pictures were taken and dates that files were created.²⁰ In addition to the information that other users, particularly a user's "friends" or "followers," may view, Facebook collects more obscure information that "friends" and "followers" cannot access. This hidden information includes the types of content that users engage with; payment information; network, device, and connection information; and cookie data.²¹ Because of the significance of this inaccessible information, this Section now expounds upon each of these categories in turn.

First, Facebook collects information about the types of content with which its users interact.²² Facebook uses much of this data to tailor content and advertising to individual users.²³ For example, Facebook maintains a list of advertisement topics that it may target against a particular user based on that user's "likes, interests and other data."²⁴ Similarly, Facebook curates a collection of Facebook Watch topics to show users relevant videos based on their interaction history with previous videos and pages they have "liked."²⁵

¹⁹ See *Data Policy*, *supra* note 4 ("We collect the content, communications and other information you provide when you use our Products, including when you sign up for an account, create or share content, and message or communicate with others."). Facebook also allows its users to provide information in their profile relating to significant life events, political and religious views, philosophical beliefs, and racial or ethnic origin. *Id.* Sharing this information is optional, and even if users choose to provide this information to Facebook, they can restrict who may view it. *Id.*

²⁰ *Id.*

²¹ *Id.*

²² See *What Categories of My Facebook Data Are Available to Me?*, *supra* note 6 (explaining that Facebook collects a user's recent activities; searches; active sessions, meaning "date, time, device, IP address, machine cookie and browser information"; recently viewed ads; recently read articles; how many times a user visits the site's Dating, Marketplace, and Events sections; recently visited event pages; recently watched live videos; the number of times a user interacts with Facebook groups; games played; pages and people a user recently viewed; and videos watched, including the amount of time spent watching particular videos).

²³ See *Data Policy*, *supra* note 4 (explaining that Facebook uses the information that it collects to provide personalized content and features to users' timelines, make suggestions, and effectively tailor advertisements and other sponsored content).

²⁴ *What Categories of My Facebook Data Are Available to Me?*, *supra* note 6.

²⁵ *Id.* Facebook also curates a similar collection of topics for a user's News Feed. *Id.*

Second, Facebook also collects information pertaining to users' network, device, and connection information.²⁶ The site records recent activity from a user's specific IP address, including message activity, payment activity, logins, active sessions, pages visited, and logouts.²⁷ This information also helps Facebook to detect whether a device may be a bot.²⁸ Furthermore, Facebook collects information from devices such as Bluetooth signals, nearby Wi-Fi points, and nearby cell towers.²⁹ If a user has the device location settings turned on, Facebook also collects data from GPS locations.³⁰ Facebook uses this information to provide users with content relevant to their locality and in their language and to make suggestions based on a user's current location, such as nearby events.³¹

Third, Facebook extensively retains cookie data from cookies stored on a user's device.³² Facebook defines cookies as "small pieces of text used to store information on web browsers" and "to store and receive identifiers and other information on computers, phones and

²⁶ *Data Policy*, *supra* note 4.

²⁷ *What Categories of My Facebook Data Are Available to Me?*, *supra* note 6; see also *Facebook, Social Media Privacy, and the Use and Abuse of Data: Joint Hearing Before the S. Comm. on Com., Sci. & Transp. and the S. Comm. on the Judiciary*, 115th Cong. 26 (2018) [hereinafter *Facebook Data Hearing*] (statement of Mark Zuckerberg, Chairman and CEO, Facebook, Inc.) (noting that it is common to collect website user information). Facebook also collects the unique identification numbers of devices used to log onto Facebook, the country and language of those devices, and the user's most recent location recorded by the devices. *What Categories of My Facebook Data Are Available to Me?*, *supra* note 6. In addition, Facebook collects device attributes such as signal strength, browser type, hardware and software versions, and available storage. *Data Policy*, *supra* note 4.

²⁸ *Facebook Data Hearing*, *supra* note 27, at 26 (stating that Facebook collects device information to look for signs that a device is a bot or that an account is inauthentic). "Bots are large numbers of automated accounts controlled by single users." *Bots Blamed for COVID Misinformation on Facebook*, U.S. NEWS & WORLD REP. (June 7, 2021), <https://www.usnews.com/news/health-news/articles/2021-06-07/bots-blamed-for-covid-misinformation-on-facebook>. Bots can repeatedly share Facebook posts to influence users with misinformation. *Id.*

²⁹ *Data Policy*, *supra* note 4.

³⁰ *Id.*

³¹ See *Data Policy*, *supra* note 4 ("We use the information we have (subject to choices you make) . . . [to p]rovide measurement, analytics, and other business services . . . [, p]romote safety, integrity and security . . . [, c]ommunicate with you . . . [and r]esearch and innovate for social good.").

³² *Id.*

other devices.”³³ Cookies allow Facebook to track user activity, including when users are logged in and the browser from which a user accesses Facebook.³⁴ Facebook places cookies on individuals’ computers or devices and receives information that is stored in cookies when individuals use Facebook products, third-party applications, and websites that use Facebook products and technologies.³⁵ Facebook uses cookies if a person has a Facebook account and uses Facebook products so that Facebook can better understand the information that it receives from users, including information about their use of third-party applications and websites.³⁶

Whenever a person visits an application or a website that features Facebook technologies—including the Facebook “comment” or “like” buttons—Facebook “automatically log[s] (i) standard browser or app records of the fact that a particular device or user visited the website or app . . . and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person’s activities on that site.”³⁷ Millions of websites feature the Facebook “like” button, and hundreds of millions of webpages include the Facebook “share” button.³⁸ Because third-party applications and websites using Facebook’s features do not know whether an individual is logged into Facebook when they visit their pages, Facebook even receives information from these pages about individuals who are logged out or do not have a Facebook

³³ *Cookies & Other Storage Technologies*, FACEBOOK, <https://www.facebook.com/policies/cookies/> (last visited Jan. 29, 2022). Facebook uses cookies to help verify accounts; determine when users are logged in; keep users’ accounts, data, and Facebook products secure and safe; show tailored advertisements; provide better functionality and performance; and to create analytics for research; among other purposes. *Id.*

³⁴ See @Seralathan, *Facebook Cookies Analysis*, MEDIUM (Mar. 14, 2019), <https://medium.com/@TechExpertise/facebook-cookies-analysis-e1cf6ffbf8a> (identifying and describing some of the more important cookies that Facebook uses).

³⁵ See *id.* (explaining where Facebook uses cookies); *Facebook Data Hearing*, *supra* note 27, at 255 (statement of Mark Zuckerberg, Chairman and CEO, Facebook, Inc.) (stating that Facebook servers automatically log people’s cookies when they visit websites and apps that feature Facebook technologies, including the Facebook “like” and “comment” buttons).

³⁶ *Cookies & Other Storage Technologies*, *supra* note 33.

³⁷ *Facebook Data Hearing*, *supra* note 27, at 255 (statement of Mark Zuckerberg, Chairman and CEO, Facebook, Inc.).

³⁸ *Id.*

profile.³⁹ Facebook purports, however, that it does not use cookies to maintain profiles of non-Facebook users.⁴⁰ This is a small number of people, though, since more than three billion individuals globally have Facebook accounts.⁴¹

III. BACKGROUND ON THE FOURTH AMENDMENT

A. DEFINING A “SEARCH” UNDER THE FOURTH AMENDMENT

The Fourth Amendment protects “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.”⁴² The essential purpose of the Fourth Amendment “is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials.”⁴³ Historically, to determine whether a government action constituted a Fourth Amendment search, courts used a trespass analysis that asked whether the government physically intruded onto an area protected by the U.S. Constitution to obtain the information at issue.⁴⁴ Today, however, courts also inquire into a person’s

³⁹ See David Baser, *Hard Questions: What Data Does Facebook Collect When I’m Not Using Facebook, and Why?*, META (Apr. 16, 2018), <https://about.fb.com/news/2018/04/data-off-facebook/> (“When you visit a site or app that uses our services, we receive information even if you’re logged out or don’t have a Facebook account. This is because other apps and sites don’t know who is using Facebook.”); see also *What Information Does Facebook Get When I Visit a Site with the Like Button?*, FACEBOOK, <https://www.facebook.com/help/186325668085084> (last visited Jan. 29, 2022) (stating that individuals who visit a site with a Facebook plugin that do not have Facebook accounts send Facebook “a more limited set of info”). “[P]lugins, like the Like button, the Share button and comments, are tools that let you share your experiences on other websites with your friends on Facebook.” *How do Social Plugins Work on Facebook?*, FACEBOOK, <https://www.facebook.com/help/203587239679209> (last visited Jan. 29, 2022).

⁴⁰ See *Facebook Data Hearing*, *supra* note 27, at 299 (statement of Mark Zuckerberg, Chairman and CEO, Facebook, Inc.) (“We do not use web browsing data to show ads to non-users or otherwise store profiles about non-users.”).

⁴¹ See *Company Info*, FACEBOOK, <https://about.fb.com/company-info/> (last visited Jan. 29, 2022) (stating the number of Facebook users around the world); Statista Rsch. Dep’t, *supra* note 3 (stating that Facebook had over 2.85 billion active monthly users in 2020).

⁴² U.S. CONST. amend. IV.

⁴³ *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018) (quoting *Camara v. Mun. Ct.*, 387 U.S. 523, 528 (1967)).

⁴⁴ See *Boyd v. United States*, 116 U.S. 616, 622 (1886) (holding that “a compulsory production of a man’s private papers to establish a criminal charge against him” violates the

reasonable expectation of privacy to determine when a search occurs for Fourth Amendment purposes.⁴⁵ Thus, the inquiry for whether the Fourth Amendment protects a person's expectation of privacy from government searches turns on reasonableness.⁴⁶

The U.S. Supreme Court established that “the Fourth Amendment protects people, not places” in *Katz v. United States*.⁴⁷ In *Katz*, FBI agents attached a device to the outside of a public telephone booth that Petitioner Katz used to transmit wagers to individuals in other cities.⁴⁸ The Court held that the FBI agents violated Katz's “privacy upon which he justifiably relied” while using the phone booth.⁴⁹ While the *Katz* majority used an expectation-of-privacy analysis, Justice Harlan's concurrence offered a two-part inquiry for determining when a Fourth Amendment search occurs, stating that the Fourth Amendment affords protection when a person displays an actual expectation of privacy and when “society is prepared to recognize” that expectation as a reasonable one.⁵⁰ In later cases, the Court adopted Justice Harlan's two-part inquiry as the leading test to determine whether a search occurred.⁵¹

Fourth Amendment under a trespass analysis); *Olmstead v. United States*, 277 U.S. 438, 464 (1928) (finding that wiretapping telephone wires on a public street did not constitute a Fourth Amendment search because the government did not enter into the defendants' offices or houses), *overruled by Katz v. United States*, 389 U.S. 347 (1967), and *Berger v. New York*, 388 U.S. 41 (1967); *see also United States v. Jones*, 565 U.S. 400, 405 (2012) (noting that this trespass inquiry was the test “at least until the latter half of the 20th century” (first citing *Kyllo v. United States*, 533 U.S. 27, 31 (2001); and then citing Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004))).

⁴⁵ *See Katz*, 389 U.S. at 361 (Harlan, J., concurring) (defining a reasonable expectation of privacy approach to determine whether a Fourth Amendment search occurred); *e.g.*, *Riley v. California*, 573 U.S. 373, 381–82 (2014) (adopting the reasonable expectation of privacy test).

⁴⁶ *See Riley*, 573 U.S. at 381–82 (“[T]he ultimate touchstone of the Fourth Amendment is ‘reasonableness.’” (quoting *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006))).

⁴⁷ *Katz*, 389 U.S. at 351 (majority opinion).

⁴⁸ *Id.* at 348.

⁴⁹ *Id.* at 353.

⁵⁰ *Id.* at 361 (Harlan, J., concurring).

⁵¹ *See, e.g.*, *California v. Ciraolo*, 476 U.S. 207, 211, 213–15 (1986) (adopting the two-part inquiry to hold that a search did not occur when police officers flew a plane over the respondent's house and saw marijuana plants growing in the yard); *Smith v. Maryland*, 442 U.S. 735, 737, 740–42 (1979) (applying Justice Harlan's *Katz* analysis to hold that the petitioner did not have “a ‘legitimate expectation of privacy’ regarding the numbers he dialed

B. THE PRIVATE SEARCH DOCTRINE

Under the private search doctrine, the government may reconstruct a search previously performed by a private party without first obtaining a warrant.⁵² Because the Fourth Amendment applies only to government searches, private individuals may conduct searches of their own.⁵³ The private search doctrine arises from the U.S. Supreme Court's opinion in *United States v. Jacobsen*.⁵⁴ The *Jacobsen* Court held that a subsequent government search of a package containing a white, powdery substance did not violate the Fourth Amendment because FedEx employees had previously searched the same container.⁵⁵ There, the doctrine allowed the government to reconstruct a private search—even where the contents were not necessarily in plain view—when it was virtually certain that the inspection would not tell the government anything more than what the private search already revealed.⁵⁶ The scope of the government search was limited to the physical container that was searched by the private party.⁵⁷ Thus, *Jacobsen* held that a subsequent government search does not violate the Fourth Amendment because the owner holds “no legitimate

on his phone” that were recorded by a pen register installed by the telephone company). Notably, the reasonable-expectation-of-privacy test does not displace the property-based test but is rather an addition to that test. *See United States v. Jones*, 565 U.S. 400, 409 (2012) (“[T]he *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test.”).

⁵² *See United States v. Jacobsen*, 466 U.S. 109, 119 (1984) (holding that an individual has no privacy interest in a package that was previously examined by a private party).

⁵³ *See id.* at 113 (explaining that the Fourth Amendment does not regulate private conduct).

⁵⁴ *See id.* at 126 (“[T]he federal agents did not infringe any constitutionally protected privacy interest that had not already been frustrated as the result of private conduct.”).

⁵⁵ *See id.* at 119–20 (“The agent’s viewing of what a private party had freely made available for his inspection did not violate the Fourth Amendment.”).

⁵⁶ *See id.* at 118–19 (“Even if the white powder was not itself in ‘plain view’ because it was still enclosed in so many containers and covered with papers, there was a virtual certainty that nothing else of significance was in the package and that a manual inspection of the tube and its contents [by the Drug Enforcement Administration agent] would not tell him anything more than he already had been told.”).

⁵⁷ *See id.* at 119 (explaining that the respondents had no privacy interest in the contents of the package because it remained unsealed and because FedEx employees had examined it before the government viewed its contents).

expectation of privacy” in contents already searched by a private party.⁵⁸

Jacobsen limits the application of the private search doctrine in many respects. First, the private party that initially conducts the search must reveal its findings to the government before the government may conduct its own search.⁵⁹ Second, as mentioned above, the government’s subsequent search may not go beyond the scope of the private party’s initial search.⁶⁰ Meeting this requirement means that the government must have “virtual certainty” that its subsequent search will not reveal anything more than what the initial private search already revealed.⁶¹ Third, some courts applying *Jacobsen* hold that the private search doctrine does not apply when the search is of a hotel room.⁶² Since *Jacobsen*, the influence of technology has prompted disagreement over what constitutes a “search” in the digital context, particularly when private technology companies collect and have the ability to search through vast amounts of personal information.⁶³

C. THE UNCERTAINTY OF THE STORED COMMUNICATIONS ACT

Also relevant to a user’s privacy interest in information stored online is the Stored Communications Act (SCA).⁶⁴ Enacted in 1986, Congress intended for the SCA to provide privacy protections to

⁵⁸ *Id.* at 120.

⁵⁹ *See id.* at 117 (“It is well-settled that when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities The Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated.”); *see also* *United States v. D’Andrea*, 648 F.3d 1, 8 (1st Cir. 2011) (explaining that the private search doctrine follows from a private party revealing private information to the government).

⁶⁰ *Jacobsen*, 466 U.S. at 117.

⁶¹ *See D’Andrea*, 648 F.3d at 9 (“[A]n antecedent private search does not amount to a free pass for the government to rummage through a person’s effects.”).

⁶² The Sixth Circuit, for example, has applied this principle. *See, e.g.*, *United States v. Allen*, 106 F.3d 695, 699 (6th Cir. 1997) (declining to extend the private search doctrine to the private search of motel rooms); *United States v. Spicer*, 432 F. App’x 522, 524 (6th Cir. 2011) (declining to extend the private search doctrine to hotel rooms).

⁶³ *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 537 (2005) (identifying the difficulty of applying the Fourth Amendment “to the retrieval of data” from computers). For further discussion, see *infra* Section III.C.

⁶⁴ 18 U.S.C. §§ 2701–13.

computer communications that were not covered by the traditional trespass analysis of the Fourth Amendment.⁶⁵ Section 2702 of the SCA prohibits entities providing electronic communication service or remote computing service to the public from voluntarily divulging the contents of communications “in electronic storage” or “carried or maintained on that service” “to any person or entity,” as well as “a[ny] record or other information pertaining to a subscriber to or customer of such service . . . to any governmental entity.”⁶⁶

It is unclear whether and to what extent the SCA applies to modern technology, such as Facebook, due to the statute’s archaic understanding of technology.⁶⁷ For example, the statute only applies to entities that provide electronic communication services (ECS) or remote computing services (RCS), but a provider can act as an RCS in one instance, an ECS in another instance, and as neither in others.⁶⁸ It is also unclear whether social media is governed by the SCA’s ECS or RCS provisions.⁶⁹ On top of this, the SCA’s prohibition on voluntary disclosure of a user’s information only pertains to information related to content, meaning “communication that a person wishes to share or communicate with another person.”⁷⁰ The SCA’s provision regarding “a record or other information pertaining to a subscriber to or customer of such service”⁷¹ refers to non-content information, which is defined as “information about the communication that the network uses to deliver and process the content information.”⁷² Thus, the SCA’s

⁶⁵ See Orin S. Kerr, *A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1208–13 (2004) [hereinafter Kerr, *A User’s Guide*] (explaining why Congress enacted the SCA).

⁶⁶ 18 U.S.C. § 2702(a)(1)–(3).

⁶⁷ See Christopher J. Borchert, Fernando M. Pinguelo & David Thaw, *Reasonable Expectations of Privacy Settings: Social Media and the Stored Communications Act*, 13 DUKE L. & TECH. REV. 36, 45–46 (2015) (explaining how the language of the SCA, which was “drafted in the 1980s, fail[s] to provide an easily adaptable framework,” especially for technology that does not fit neatly within its language).

⁶⁸ See Kerr, *A User’s Guide*, *supra* note 65, at 1215 (“The classifications of ECS and RCS are context sensitive: the key is the provider’s role with respect to a particular copy of a particular communication, rather than the provider’s status in the abstract.”).

⁶⁹ See Borchert et al., *supra* note 67, at 57 (noting the SCA’s lack of clarity regarding protection of social media users).

⁷⁰ Kerr, *A User’s Guide*, *supra* note 65, at 1228.

⁷¹ 18 U.S.C. § 2702(a)(3).

⁷² Kerr, *A User’s Guide*, *supra* note 65, at 1228.

prohibitions might not apply when an individual uses Facebook for noncommunicative purposes, such as browsing different pages or scrolling through a timeline.

Scholars have called for Congress to amend the SCA to apply the language more clearly to modern technology.⁷³ As the SCA currently stands, courts disagree about how to apply the statute to new technologies such as Facebook.⁷⁴ While scholars and courts debate how the SCA applies to this information and what can be done to amend it, this Note argues that the Court's current Fourth Amendment jurisprudence prohibits disclosure of non-public Facebook information to police without needing to point to any particular statute.

D. THE INFLUENCE OF TECHNOLOGY ON THE FOURTH AMENDMENT AND THE PRIVATE SEARCH DOCTRINE

Advances in technology have forced courts to re-tool their Fourth Amendment jurisprudence. Starting in *Katz*, the U.S. Supreme Court extended the reasonable-expectation-of-privacy analysis to protect individuals from unreasonable government searches in areas where the historical trespass-based analysis would otherwise have not.⁷⁵ The Fourth Amendment protects individuals from physical *and* electronic intrusions into a place where an individual exhibits a subjective expectation of privacy and where that expectation is reasonable.⁷⁶ As technology has made it easier for the government to surveil areas that were once thought of as private,

⁷³ *E.g.*, Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 419 (2014) (arguing that sweeping reform to the SCA and other privacy laws is necessary because “[t]oday’s Internet has diverged in profound ways from the Internet that existed when Congress last enacted major reform”); Borchert et al., *supra* note 67, at 65 (“[T]his Article suggests Congress amend the SCA in order to ensure the Act achieves its original intent . . . [and] further recommends Congress adopt technology-neutral statutory language to more effectively protect communications content now and in the future.”).

⁷⁴ *See* Borchert et al., *supra* note 67, at 48, 53 (noting that courts disagree over whether an internet service provider “is acting as a provider of ECS or RCS with regard to a particular communication” and which communications made on social networking platforms receive SCA protection).

⁷⁵ *See supra* notes 45–50 and accompanying text.

⁷⁶ *See Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring) (“[E]lectronic as well as physical intrusion into a place that is in this sense private may constitute a violation of the Fourth Amendment . . .”).

the Court has acted to “assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.”⁷⁷ The Court has used this reasoning to prohibit the government from using technology not readily made available to the public, such as thermal imagers, to explore what occurs within an individual’s home without a warrant.⁷⁸

Cell phones and GPS have further complicated Fourth Amendment jurisprudence. The U.S. Supreme Court noted in *Riley v. California* that cell phones have become “a pervasive and insistent part of daily life,” and “a significant majority of American adults now own such phones.”⁷⁹ Due to the vast amounts of personal information contained in cell phones, officers generally must obtain a warrant before conducting a search of one.⁸⁰ Cell phones feature immense storage capacity and can store many different kinds of information.⁸¹ These capabilities make it possible to reconstruct “[t]he sum of an individual’s private life” through information that dates back to when the phone was purchased, and as is often the case, even earlier.⁸² Similarly, in *United States v. Jones*, the U.S. Supreme Court held that placing a GPS tracker on a car for twenty-eight days constituted a Fourth Amendment search.⁸³ Although the *Jones* majority used a trespass analysis to conclude that the

⁷⁷ *Kyllo v. United States*, 533 U.S. 27, 34 (2001).

⁷⁸ *See id.* at 35–36 (reasoning that allowing the government to use a thermal imager on petitioner’s home to measure heat radiating from its side and roof “would leave the homeowner at the mercy of advancing technology—including imaging technology that could discern all human activity in the home”).

⁷⁹ *Riley v. California*, 573 U.S. 373, 385 (2014).

⁸⁰ *See id.* at 386 (“Cell phones, however, place vast quantities of personal information literally in the hands of individuals.”). The *Riley* Court likened the government’s argument that data stored on a cell phone is virtually the same as other physical items to “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.” *Id.* at 393. Privacy concerns implicated in the data stored on cell phones go far beyond those implicated by the search of physical items. *Id.*

⁸¹ *See id.* at 394 (“Even the most basic phones that sell for less than \$20 might hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on.”).

⁸² *See id.* at 394–95 (describing the consequences that cell phone data presents for privacy). Data such as browsing history, location information, and applications that manage a person’s detailed information all make it easy for third parties to learn the most intimate details of a person’s life from a cell phone alone. *Id.* at 395–96.

⁸³ 565 U.S. 400, 403–04 (2012).

government conducted a search under the meaning of the Fourth Amendment,⁸⁴ a “shadow majority” made up of Justice Alito and the three Justices who joined his concurring opinion (Justices Ginsburg, Breyer, and Kagan), plus Justice Sotomayor who concurred alone,⁸⁵ concluded that the GPS data became something more than mere location data because of the large amount of information collected and the inferences that the government could make from it.⁸⁶ The five concurring Justices in *Jones*—especially Justice Sotomayor—touched on a “mosaic approach” to the Fourth Amendment, which focuses on the aggregated sum of an individual’s public movements that GPS monitoring entails.⁸⁷ Justice Sotomayor suggested that individuals do not reasonably expect that the government would aggregate their individual movements, which would allow the government to gather substantial information about a person’s private life.⁸⁸

⁸⁴ See *id.* at 404–05 (“The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a ‘search’ within the meaning of the Fourth Amendment when it was adopted.”).

⁸⁵ Margot E. Kaminski, Response, *Carpenter v. United States: Big Data is Different*, GEO. WASH. L. REV.: ON THE DOCKET (July 2, 2018), <https://www.gwlr.org/carpenter-v-united-states-big-data-is-different>.

⁸⁶ See *Jones*, 565 U.S. at 430 (Alito, J., concurring) (“[T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society’s expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual’s car for a very long period.”); *id.* at 415 (Sotomayor, J., concurring) (“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.”).

⁸⁷ See Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 320 (2012) [hereinafter Kerr, *The Mosaic Theory*] (“The mosaic theory requires courts to apply the Fourth Amendment search doctrine to government conduct as a collective whole rather than in isolated steps. Instead of asking if a particular act is a search, the mosaic theory asks whether a series of acts that are not searches in isolation amount to a search when considered as a group.”).

⁸⁸ See *Jones*, 565 U.S. at 415–16 (Sotomayor, J., concurring) (detailing the extent of information gathered by GPS monitoring, such as “familial, political, professional, religious, and sexual associations”); see also Kerr, *The Mosaic Theory*, *supra* note 87, at 328 (“Justice Sotomayor focuses on whether a person has Fourth Amendment rights ‘in the sum’ of their public movements, rather than in individual movements. . . . Justice Sotomayor [also] asks whether people reasonably expect that their movements not only will be recorded but also ‘aggregated.’”).

In 2018, the U.S. Supreme Court cemented its prior reasoning from *Riley v. California*⁸⁹ and Justice Sotomayor’s reasoning from *Jones in Carpenter v. United States*.⁹⁰ *Carpenter* involved an individual suspected of robbing Radio Shack and T-Mobile stores.⁹¹ After another suspect identified Carpenter as an accomplice in the robberies, prosecutors applied for Carpenter’s phone records under the SCA, which features a standard lower than the probable cause threshold usually needed to obtain this information.⁹² From the prosecutors’ granted SCA application, federal magistrate judges ordered MetroPCS and Sprint—two wireless carriers Carpenter used—to disclose cell site location information (CSLI) for Carpenter’s cell phone for the four-month period in which the robberies occurred.⁹³ MetroPCS “produced records spanning 127 days,” and Sprint “produced two days of records,” culminating in the government obtaining “12,898 location points cataloging Carpenter’s movements.”⁹⁴ The government used this information to charge and convict Carpenter at trial, and the U.S. Court of Appeals for the Sixth Circuit affirmed the conviction.⁹⁵

The government in *Carpenter* argued that the third-party doctrine⁹⁶ applied to Carpenter’s CSLI records.⁹⁷ Similar to the

⁸⁹ 573 U.S. 373 (2014).

⁹⁰ See 138 S. Ct. 2206, 2217–18 (2018) (explaining that the collected data from the cell phone location records at issue contravened the privacy expectation set out in *Riley* and presented an even larger privacy concern than the data considered in *Jones*); see also Kaminski, *supra* note 85 (“[T]he central move in *Carpenter* stems from Justice Sotomayor’s opinion in *Jones* and Chief Justice Roberts’s opinion in *Riley*.”).

⁹¹ *Carpenter*, 138 S. Ct. at 2212.

⁹² *Id.* at 2212–13. The Court noted that the SCA “permits the Government to compel the disclosure of certain telecommunications records when it ‘offers specific and articulable facts showing that there are reasonable grounds to believe’ that the records sought ‘are relevant and material to an ongoing criminal investigation.’” *Id.* at 2212 (quoting 18 U.S.C. § 2703(d)).

⁹³ *Id.* at 2212.

⁹⁴ *Id.*

⁹⁵ *Id.* at 2212–13. The Sixth Circuit reasoned that Carpenter did not have a reasonable expectation of privacy in the CSLI because he voluntarily conveyed that information to his wireless carriers. *Id.* at 2213.

⁹⁶ See *United States v. Miller*, 425 U.S. 435, 443 (1976) (explaining that the third-party doctrine states that an individual “takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government”).

⁹⁷ See *Carpenter*, 138 S. Ct. at 2219 (“The Government’s primary contention . . . is that the third-party doctrine governs this case. In its view, cell-site records are fair game because they are ‘business records’ created and maintained by the wireless carriers.”).

private search doctrine, the third-party doctrine states that an individual maintains no reasonable expectation of privacy in information that is voluntarily conveyed to third parties.⁹⁸ The Court disagreed with the government's argument and explained that "the seismic shifts in digital technology" allow wireless carriers to track Carpenter's, and everyone else's, location for many years, which brings this case outside of the outdated third-party doctrine framework.⁹⁹ Unlike typical witnesses, entities such as Sprint "are ever alert, and their memory is nearly infallible."¹⁰⁰ Furthermore, the Court reasoned that CSLI is not necessarily "shared" because cell phones have become such an integral, indispensable part of everyday life.¹⁰¹ Thus, individuals may preserve a reasonable expectation of privacy and maintain their Fourth Amendment protection in some circumstances in which a third party possesses their private information.¹⁰² In these situations, the government's intrusion on privacy damages everyone, not just those under investigation.¹⁰³

IV. EXCLUDING THE PRIVATE SEARCH DOCTRINE FROM FACEBOOK DATA

The Court's reasoning in *Carpenter* logically extends to Facebook data that is not readily made available to the public. Although this information is conveyed to Facebook, social media users maintain a

⁹⁸ See *Miller*, 425 U.S. at 443 ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.").

⁹⁹ *Carpenter*, 138 S. Ct. at 2219.

¹⁰⁰ *Id.*

¹⁰¹ *Id.* at 2220.

¹⁰² See *id.* at 2217 ("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.").

¹⁰³ See *id.* at 2218 ("[T]he retrospective quality of the data here gives police access to a category of information otherwise unknowable. . . . Critically, because location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone. . . . Only the few without cell phones could escape this tireless and absolute surveillance.").

reasonable expectation of privacy in data that other Facebook users—including “friends”—cannot access.¹⁰⁴ Further, this expectation is reasonable and, like CSLI data, is not voluntarily conveyed.¹⁰⁵ This Part begins by drawing similarities between the data obtained by the government in *Jones*, *Carpenter*, and other cases and the data collected by Facebook. Next, Section IV.B suggests that information collected by Facebook has the potential to warrant even greater privacy concerns than those in *Jones* and *Carpenter* if that information becomes available to law enforcement. Last, Section IV.C argues that the private search doctrine should be excluded from the Facebook data collection context and proposes a bright-line rule for when a warrant should be required to obtain this information.

A. REASONABLE EXPECTATION OF PRIVACY IN FACEBOOK DATA

A majority of the U.S. Supreme Court seems prepared to recognize an expectation of privacy in Facebook data due to that data’s comprehensiveness and the type of information it reveals about its users. The *Jones* shadow majority supported an expectation of privacy in the comprehensiveness of certain types of information sought.¹⁰⁶ In his concurrence, Justice Alito stated that society has an expectation that the government will not—and cannot—“secretly monitor and catalogue [an individual’s] every single movement” for an extended period.¹⁰⁷ Justice Sotomayor expanded on this idea by positing that data collected by methods such as GPS monitoring create an extensive “record of a person’s public movements that reflects a wealth of detail about her familial,

¹⁰⁴ See, e.g., *Davis v. Facebook, Inc. (In re Facebook, Inc. Internet Tracking Litig.)*, 956 F.3d 589, 603–04, 606 (9th Cir. 2020) (concluding that Plaintiffs pleaded a reasonable expectation of privacy in their Facebook data sufficient to survive a Rule 12(b)(6) motion to dismiss when Plaintiffs alleged that Facebook “compiled highly personalized profiles from sensitive browsing histories and habits”).

¹⁰⁵ See *id.* at 603 (describing Facebook’s alleged data collection methods as “surreptitious and unseen”).

¹⁰⁶ See Kaminski, *supra* note 85 (stating that the *Jones* shadow majority recognized that “more sophisticated, pervasive, persistent surveillance of location data” is qualitatively different than other modes of surveillance and reveals sensitive information that warrants Fourth Amendment protection).

¹⁰⁷ *United States v. Jones*, 565 U.S. 400, 430 (2012) (Alito, J., concurring).

political, professional, religious, and sexual associations.”¹⁰⁸ The Fourth Amendment does not protect general location information that is uncontextualized; rather, it protects against the collection of private and detailed information in the aggregate that goes beyond what a single record could reveal.¹⁰⁹ In *Carpenter*, the Court also supported an expectation of privacy concerning detailed, aggregated information compiled every day over a span of several years.¹¹⁰

Similar to GPS monitoring or CSLI that can track an individual’s movements precisely, Facebook compiles detailed information about its users that, in the aggregate, presents an even greater privacy concern than the information collected in *Jones* and *Carpenter* did.¹¹¹ Since its inception in 2004, Facebook has changed the way society communicates: much of what was once done by letter or email, or even by face-to-face communication, is now done by posting on a “friend’s” Facebook page or sending a message through Messenger. This communication revolution has been accompanied by a seismic shift in technology that has made it easier to monitor Facebook’s millions of users.¹¹²

Facebook’s collection of location information is sufficient to trigger the Court’s concerns articulated in *Carpenter* and *Jones*. When a user logs on to Facebook, the site collects the most recent location recorded by the device used to log on.¹¹³ Furthermore, Facebook records the location of a device’s nearby Wi-Fi points and

¹⁰⁸ *Id.* at 415 (Sotomayor, J., concurring).

¹⁰⁹ *See, e.g.*, *Riley v. California*, 573 U.S. 373, 395–96 (2014) (noting that the expansive data contained in cell phones implicate greater privacy concerns than the limited information revealed by physical records); *Kyllo v. United States*, 533 U.S. 27, 34 (2001) (holding that information obtained that could not otherwise be obtained absent a physical “intrusion into a constitutionally protected area” by technology that is not generally used by the public constitutes a search protected by the Fourth Amendment (quoting *Silverman v. United States*, 365 U.S. 505, 512 (1961))); *Katz v. United States*, 389 U.S. 347, 351 (1967) (“[T]he Fourth Amendment protects people, not places.”).

¹¹⁰ *See Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018) (“Yet this case is not about ‘using a phone’ or a person’s movement at a particular time. It is about a detailed chronicle of a person’s physical presence compiled every day, every moment, over several years.”).

¹¹¹ *See* discussion *supra* Part II.

¹¹² *Compare Carpenter*, 138 S. Ct. at 2219 (noting that CSLI led to a “seismic shift[] in digital technology”), *with supra* text accompanying notes 1–5 (describing the enormous technological shift associated with Facebook’s rise in popularity).

¹¹³ *See supra* note 23 and accompanying text.

cell towers, and if the setting is turned on, a user's GPS location.¹¹⁴ A court should find that this information alone is sufficient to warrant Fourth Amendment protection. Like the CSLI at issue in *Carpenter*, Facebook's data collection practices allow the company to track its users' location for many years.¹¹⁵ And just like a wireless carrier, Facebook is always alert, and its memory as a witness is almost infallible.¹¹⁶ Although Facebook gives its users the option to turn off location services,¹¹⁷ Facebook still accesses location information to understand a user's internet connection and to enable its "check-in" and "events" features.¹¹⁸ Thus, there is no way to truly opt out of having location information collected without deleting Facebook altogether. Because the average user spends roughly one hour on Facebook per day, the location information gathered over time is substantial.¹¹⁹

But Facebook does not stop at collecting location information. Facebook also tracks recently viewed ads and articles, videos watched, the number of times a user interacts with different Groups, how many times a user has viewed the Dating and Events sections, and recently viewed items and interactions on Marketplace.¹²⁰ Compiling all of this information reveals a person's

¹¹⁴ See *supra* notes 21–22 and accompanying text.

¹¹⁵ See Aimee Picchi, *OK, You've Deleted Facebook, But Is Your Data Still Out There?*, CBS NEWS (Mar. 23, 2018, 5:00 AM), <https://www.cbsnews.com/news/ok-youve-deleted-facebook-but-is-your-data-still-out-there/> (noting that Facebook retains "log data—a record of what a user does, such as when they log in, click on a Facebook group or post a comment" indefinitely, even after a user deletes their account).

¹¹⁶ See, e.g., *supra* note 100 and accompanying text.

¹¹⁷ On iOS devices, for example, a user may set location services to "Always," "While Using," or "Never." See *Facebook and Location*, FACEBOOK, <https://www.facebook.com/help/337244676357509> (last visited Jan. 29, 2022) (describing these options further).

¹¹⁸ See *id.* ("When Location Services and Location History are turned off, we may still estimate your location using things like check-ins, events and information about your internet connection.").

¹¹⁹ See Marie Ennis-O'Connor, *How Much Time Do People Spend on Social Media in 2019?*, MEDIUM (Aug. 8, 2019), <https://medium.com/@JBBC/how-much-time-do-people-spend-on-social-media-in-2019-infographic-cc02c63bede8> (stating that people spend an average of fifty-eight minutes per day on Facebook globally). Ennis-O'Connor also notes that people spend fifty-three minutes per day on Instagram, which is noteworthy because Instagram is a subsidiary of Facebook. *Id.*; *supra* note 18.

¹²⁰ See *supra* notes 1–13 and accompanying text.

most intimate personal affairs in detail.¹²¹ Allowing the government access to this information without a warrant may allow it to see, for example, that a person has frequently viewed support pages for how to come out as gay to one's family or pages of various medical offices specializing in cancer treatment. All of this data would make it possible to reconstruct "[t]he sum of an individual's private life" through information otherwise only known by the user.¹²² Because of the detailed wealth of information that Facebook collects, access to such information by the government constitutes a search under the Court's recent opinions in *Jones*, *Riley*, and *Carpenter*.

B. EXCLUDING THE PRIVATE SEARCH DOCTRINE FROM THE COLLECTION OF FACEBOOK DATA

In *Carpenter*, the Court declined to extend the third-party doctrine to the collection of CSLI due to the "unique nature of cell phone location information."¹²³ The Court's holding relied on the fact that the location information was not truly "shared" and that "seismic shifts in digital technology" made it possible to gather much more information over a longer period of time than other surveillance methods.¹²⁴ The above Section applies the seismic-shifts-in-technology argument to Facebook information;¹²⁵ this Section focuses on the issue of voluntariness.

The *Carpenter* Court stated that CSLI is not fully voluntarily shared information.¹²⁶ First, the Court noted that cell phones have become such an integral part of everyday life that they are

¹²¹ See, e.g., *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (warning against allowing the government access to a comprehensive record of a person's movement that reveals a wealth of detailed, personal information); *Riley v. California*, 573 U.S. 373, 395–96 (2014) ("An Internet search and browsing history . . . could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD.").

¹²² See *Riley*, 573 U.S. at 394 (noting this concern regarding a cell phone's storage capacity and ability to store many different types of information).

¹²³ *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018).

¹²⁴ *Id.* at 2219–20.

¹²⁵ See discussion *supra* Section IV.A.

¹²⁶ See *Carpenter*, 138 S. Ct. at 2220 ("Cell phone location information is not truly 'shared' as one normally understands the term.").

“indispensable to participation in modern society.”¹²⁷ The “indispensable” role that cell phones play in modern society makes it less likely that individuals knowingly assume the risk that a private party will access their information.¹²⁸ The pervasive use of Facebook weighs heavily in favor of extending *Carpenter’s* reasoning to non-public Facebook information. There are 297 million Facebook users in the United States.¹²⁹ Individuals use Facebook to stay in touch with friends and family, participate in political and civic activities, read the news, and perform work-related matters.¹³⁰ Moreover, Facebook and other social media platforms have become an integral part to maintaining friendships, and even romantic relationships, among younger Americans.¹³¹ In a way, Facebook has become the modern-day public square where people go to meet others, get caught up on current events, and express their opinions.¹³² Thus, like cell phones, Facebook is so indispensable to everyday life that individuals do not knowingly

¹²⁷ *Carpenter*, 138 S. Ct. at 2220; see also *Riley*, 573 U.S. at 385 (noting that cell phones “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”).

¹²⁸ See Sarah A. Mezera, Note, *Carpenter’s Legacy: Limiting the Scope of the Electronic Private Search Doctrine*, 117 MICH. L. REV. 1487, 1498–99 (2019) (“The indispensable nature of cell phones and electronic devices in modern society decreases the likelihood that a person is knowingly assuming the risk that a third party will view their information. . . . In essence, our electronic devices have become extensions of ourselves. They follow us wherever we go and record our lives in detail.”).

¹²⁹ Compare Statista Rsch. Dep’t, *supra* note 3 (indicating there were 297 million Facebook users in the United States in 2020 and an estimated 302 million in 2021), with *Carpenter*, 138 S. Ct. at 2211 (“There are 396 million cell phone service accounts in the United States . . .”).

¹³⁰ See Lee Rainie, *Americans’ Complicated Feelings About Social Media in an Era of Privacy Concerns*, PEW RSCH. CTR. (Mar. 27, 2018), <https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/> (“[W]e have documented how social media play a role in the way people participate in civic and political activities, launch and sustain protests, get and share health information, gather scientific information, engage in family matters, perform job-related activities and get news.”).

¹³¹ See *id.* (“Teenagers are especially likely to report that social media are important to their friendships and, at times, their romantic relationships.”).

¹³² See, e.g., *Packingham v. North Carolina*, 137 S. Ct. 1730, 1737 (2017) (explaining that Facebook and other social media sites have become “what for many are the principal sources for knowing current events, checking ads for employment, speaking and listening in the modern public square, and otherwise exploring the vast realms of human thought and knowledge”).

assume the risk of a private party accessing their information by logging on to the website.

Second, the Court in *Carpenter* noted that the mobile carriers logged CSLI records without “any affirmative act [by] the user beyond powering up” the device and receiving incoming texts, calls, and other notifications.¹³³ Admittedly, Facebook does not log user records at the same level of passivity at which cell carriers log CSLI records; Facebook does, however, collect user data when users are not using Facebook and does not give users an absolute ability to avoid having their information collected while using Facebook’s services.¹³⁴ Even when a user turns off location services, Facebook still has access to that user’s location information to monitor the user’s internet connection and enable various features.¹³⁵ Additionally, Facebook’s cookies policy records information automatically without an individual visiting Facebook when that individual visits a website featuring the Facebook “like” or “share” buttons.¹³⁶ Because Facebook’s “like” button appears on over eight million websites, it is difficult to avoid websites that use Facebook.¹³⁷ Therefore, unless they delete their accounts, there is no way for Facebook users to avoid having their private information recorded by Facebook without deleting their accounts. This ubiquitous use of Facebook’s “like” and “share” buttons on websites cuts against the belief that individuals voluntarily assume the risk of private parties disclosing their information to police.¹³⁸

C. DRAWING THE LINE: WHAT INFORMATION MAY LAW ENFORCEMENT REVIEW WITHOUT FIRST OBTAINING A WARRANT?

Determining what information from Facebook law enforcement may review should turn on whether an individual has a reasonable expectation of privacy in that information.¹³⁹ To start, law

¹³³ *Carpenter*, 138 S. Ct. at 2220.

¹³⁴ *See supra* notes 29–30 & 93–94 and accompanying text.

¹³⁵ *See supra* notes 117–118 and accompanying text.

¹³⁶ *See supra* note 37 and accompanying text.

¹³⁷ *See supra* note 38 and accompanying text.

¹³⁸ *See Carpenter*, 138 S. Ct. at 2220 (making a similar argument regarding the third-party doctrine based on information gathered by CSLI because “there is no way to avoid” having that information recorded other than to disconnect one’s device from the network entirely).

¹³⁹ *See discussion supra* Section III.A (identifying this standard as the first inquiry for

enforcement may view any information that would otherwise be viewable to other Facebook users because individuals do not have any legitimate expectation of privacy in information *voluntarily* conveyed to others.¹⁴⁰ Therefore, even if people believe that all of their Facebook “friends” are loyal to them, if a “friend” turns out to be a government informant or an undercover officer and reports Facebook information that is visible to other “friends,” the police should be able to use that information. This information includes posts, private messages, “likes,” “shares,” and pages and people followed.¹⁴¹ Police departments frequently obtain this information by monitoring a person’s page or specific hashtags and by “friending” individuals from undercover accounts.¹⁴² Likewise, Facebook could report this information on its own accord without conducting a Fourth Amendment “search” because the expectation of privacy in information made available to other users is already null. These types of information differ from other, nonpublic information—such as location information, cookies, and recently visited pages—because Facebook is the only entity that can see that information.¹⁴³ In those cases, individuals maintain a reasonable expectation of privacy.

Doctrine determining when nonpublic information becomes comprehensive enough to warrant Fourth Amendment protection is

determining whether a search occurs under the Fourth Amendment).

¹⁴⁰ *Cf.* *United States v. White*, 401 U.S. 745, 749 (1971) (“[H]owever strongly a defendant may trust an apparent colleague, his expectations in this respect are not protected by the Fourth Amendment when it turns out that the colleague is a government agent regularly communicating with the authorities.” (citing *Hoffa v. United States*, 385 U.S. 293 (1966))).

¹⁴¹ *See* *United States v. Stratton*, 229 F. Supp. 3d 1230, 1241 (D. Kan. 2017) (finding that the defendant “lost any reasonable expectation of privacy” in messages sent via PlayStation Network to other users). *But see* *United States v. Chavez*, 423 F. Supp. 3d 194, 204–05 (W.D.N.C. 2019) (finding that the defendant had a reasonable expectation of privacy in any “non-public” information on Facebook, including private posts and private messages). *Chavez* invokes a broader privacy protection than this Note proposes. This Note accounts for *White* in determining reasonable expectations of privacy in social media information, but *Chavez* makes no mention of the case and only mentions *Hoffa* in passing. *Id.* at 203 n.4. Nevertheless, the *Chavez* court agrees that individuals maintain a reasonable expectation of privacy in nonpublic information on Facebook. *Id.* at 205.

¹⁴² *See* Rachel Levinson-Waldman, *Government Access to and Manipulation of Social Media: Legal and Policy Challenges*, 61 *HOW. L.J.* 523, 525–26 (2018) (identifying methods used by law enforcement to surveil social media).

¹⁴³ *See supra* notes 26–27, 32 and accompanying text.

currently underdeveloped by the courts¹⁴⁴ and will depend on how future courts answer the question. For example, is comprehensiveness determined by the amount of data collected and its accuracy or by the frequency at which the data is collected?¹⁴⁵ Regardless of which analysis is used, courts should develop and follow a bright-line rule to determine comprehensiveness, such as *Carpenter*'s seven-day rule,¹⁴⁶ because of the similarities between nonpublic information and CSLI in the breadth of information they contain, the opportunity they offer the government to reconstruct intimate details about a person's life, and the feasibility of collecting the information.

Furthermore, courts should recognize that a Fourth Amendment search occurs when multiple types of nonpublic Facebook data are disclosed to law enforcement.¹⁴⁷ This disclosure would occur, for example, when Facebook attempts to share a user's log-in location information and recently watched video history. When more than one type of private information is disclosed, individuals are at greater risk of having intimate details of their lives made available to the government than they would be if only one type of information was disclosed.¹⁴⁸ Due to this significant privacy concern, courts should deem it a Fourth Amendment search when more than one

¹⁴⁴ See Daniel de Zayas, Comment, *Carpenter v. United States and the Emerging Expectation of Privacy in Data Comprehensiveness Applied to Browsing History*, 68 AM. U. L. REV. 2209, 2213 (2019) ("Courts developed the third-party doctrine in a series of cases during the age of analog technology and left it almost undisturbed as society transitioned into the modern digital age.").

¹⁴⁵ See de Zayas, *supra* note 144, at 2248 (identifying these distinct potential modes of analysis); see also *Carpenter v. United States*, 138 S. Ct. 2206, 2212, 2219 (2018) (noting that the government obtained nearly 13,000 location points that could identify an individual's location within 50 meters); *Naperville Smart Meter Awareness v. City of Naperville*, 900 F.3d 521, 524–25 (7th Cir. 2018) (holding that collecting smart-meter data, meaning data showing "both the amount of electricity being used inside a home and when that energy is used," in intervals of fifteen minutes is a "search").

¹⁴⁶ See *Carpenter*, 138 S. Ct. at 2217 n.3 (stating that seven days of CSLI collection is a search under the Fourth Amendment).

¹⁴⁷ See *Davis v. Facebook, Inc. (In re Facebook, Inc. Internet Tracking Litig.)*, 956 F.3d 589, 604 (9th Cir. 2020) (holding that individuals have a reasonable expectation of privacy in "highly personalized profiles from sensitive browsing histories and habits" that Facebook had compiled).

¹⁴⁸ See *supra* notes 63–67 and accompanying text.

type of nonpublic Facebook data is disclosed to law enforcement, regardless of how many days the information covers.

V. ANSWERING POTENTIAL CRITICISM

Some argue that protecting this information under the Fourth Amendment will hinder law enforcement efforts.¹⁴⁹ As such, because nearly three-quarters of law enforcement agencies use social media to investigate crime,¹⁵⁰ requiring the government to obtain a warrant before reviewing this information may make it more difficult for law enforcement to investigate and arrest suspected criminals.¹⁵¹ Others argue that protecting this information presents a public safety risk because social media information can be extremely valuable for surveillance purposes.¹⁵² For example, granting law enforcement access to this information allows it to save investigatory resources and time while increasing its surveillance capacity to better protect the public.¹⁵³

These criticisms are largely unfounded. While there may be times when law enforcement will be unable to access nonpublic social media information because it lacks probable cause to obtain a warrant,¹⁵⁴ such situations would not justify the invasion of privacy

¹⁴⁹ See Orin Kerr, *Sixth Circuit Creates Circuit Split on Private Search Doctrine for Computers*, WASH. POST: THE VOLOKH CONSPIRACY (May 20, 2015), <https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/05/20/sixth-circuit-creates-circuit-split-on-private-search-doctrine-for-computers> (explaining that probable cause to obtain a warrant is not always met by the report of a private party that has already performed a search).

¹⁵⁰ See Levinson-Waldman, *supra* note 142, at 524 (“[I]n a 2016 survey of over 500 domestic law enforcement agencies, three-quarters reported that they use social media to solicit tips on crime, and nearly the same number use it to . . . gather intelligence for investigations.”).

¹⁵¹ See Benjamin Holley, Note, *Digitizing the Fourth Amendment: Limiting the Private Search Exception in Computer Investigations*, 96 VA. L. REV. 677, 712 (2010) (addressing the argument “that narrow exceptions to the warrant requirement hinder police investigation, making it more difficult to find and arrest criminals”).

¹⁵² See Christopher L. Izant, Note, *Equal Access to Public Communications Data for Social Media Surveillance Software*, 31 HARV. J.L. & TECH. 237, 237–38 (2017) (“[T]he ability to view and organize [social media surveillance] data [by law enforcement] at the developer level is essential to capture the maximum intelligence value of social media communications.”).

¹⁵³ See *id.* at 238–39 (stating that social media can expose potential public safety threats and allow agencies to respond quickly, while at the same time reducing resources expended on surveillance).

¹⁵⁴ See *Illinois v. Gates*, 462 U.S. 213, 231 (1983) (stating that probable cause is met when

that would ensue. Requiring a warrant based on probable cause in these situations ensures that the question of whether access to the information should be allowed is determined by a neutral and detached magistrate judge, rather than by a police officer with hurried judgment,¹⁵⁵ or even the judgment of an algorithm developed by Facebook.¹⁵⁶ Further, there are other sources of information available for the government to investigate crimes that provide similar relevant information, such as surveillance cameras, eyewitnesses, and individual informants. Due to the wealth of personal information contained in nonpublic social media data, an individual's privacy interest should outweigh the interest of law enforcement in obtaining this information without a warrant.

Likewise, it is unclear how useful nonpublic social media information is in preventing crime and mitigating public safety risks. Law enforcement may still access public information such as social media posts, followed or "liked" pages, and group membership without obtaining a warrant.¹⁵⁷ For example, in 2019, the U.S. Attorney's Office in Southern Florida arrested and charged a Florida man based on FBI surveillance of his "violent, misogynistic and extremist social media posts and messages" that led the FBI to the man's plan to coordinate an ISIS attack against deans at two colleges he previously attended.¹⁵⁸ Also in 2019, a woman in Wisconsin pleaded guilty to crimes related to using Facebook accounts to "pledge [her] allegiance to ISIS, recruit new members for the terrorist group," and encourage individuals to engage in

there is a likelihood of criminal activity based on the "factual and practical considerations" (quoting *Brinegar v. United States*, 338 U.S. 160, 175 (1949)).

¹⁵⁵ See *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319, 326 (1979) ("We have repeatedly said that a warrant authorized by a neutral and detached judicial officer is 'a more reliable safeguard against improper searches than the hurried judgment of a law enforcement officer 'engaged in the often competitive enterprise of ferreting out crime.'") (quoting *United States v. Chadwick*, 433 U.S. 1, 9 (1977)).

¹⁵⁶ See *supra* notes 8–10.

¹⁵⁷ Any reasonable expectation of privacy in this information by a user is null because it is already viewable by their Facebook "friends." See *supra* notes 140–142 and accompanying text.

¹⁵⁸ Kim Bellware, *A Man Plotted an ISIS Attack in Revenge for Getting Kicked Out of College in Florida, Authorities Say*, WASH. POST (Nov. 27, 2019), <https://www.washingtonpost.com/education/2019/11/26/man-plotted-an-isis-attack-revenge-getting-kicked-out-college-authorities-say/>.

terrorism.¹⁵⁹ Such surveillance is permissible under the rule outlined above because police only accessed information that was viewable to other users. Even if Facebook automatically disclosed this information to law enforcement (instead of law enforcement obtaining the information on its own), this practice would not constitute a Fourth Amendment search.

Furthermore, the exigent circumstance exception to the warrant requirement will apply if the public safety threat is credible enough.¹⁶⁰ The exigent circumstance exception applies when law enforcement has “the need to prevent the imminent destruction of evidence in individual cases, to pursue a fleeing suspect, and to assist persons who are seriously injured or are threatened with imminent injury.”¹⁶¹ Thus, even with the robust warrant requirement proposed here, exceptions apply to help law enforcement and ensure public safety.

VI. CONCLUSION

If Facebook discloses information to law enforcement that is not available to other users, courts should protect such information because of its potential to reveal a mosaic of an individual’s life. Unlike other information available under the private search doctrine, disclosure of this information is not truly voluntary. The Court’s reasoning in *Carpenter* and the shadow majority’s reasoning in *Jones* logically extend to protect an individual’s privacy interest in nonpublic Facebook information under the Fourth Amendment. As such, courts should exclude this information from the private search doctrine and hold that it may not be viewed by law enforcement absent a warrant.

¹⁵⁹ Liam Stack, *Wisconsin Woman Used Hacked Facebook Accounts to Recruit for ISIS*, *Prosecutors Say*, N.Y. TIMES (Apr. 22, 2019), <https://www.nytimes.com/2019/04/22/us/wisconsin-woman-isis.html>.

¹⁶⁰ See *Riley v. California*, 573 U.S. 373, 402 (2014) (stating that the exigent circumstance exception applies when the urgency of a situation makes law enforcement’s needs so compelling that a warrantless search becomes “objectively reasonable” (quoting *Kentucky v. King*, 563 U.S. 452, 460 (2011))).

¹⁶¹ *Id.*

