

NOTE

Digital Curtilage and the Reasonable Expectation of Privacy

Brian Zilberberg*

ABSTRACT

Although the development of modern technology has impacted and enhanced the lives of average consumers, it has also presented numerous unexpected legal challenges and considerations. These new challenges have made it difficult for many antiquated laws to adequately address the modern legal problems that have emerged with new technology. Of the many growing pains discovered, privacy concerns reign as a dominant issue affecting all citizens across the United States. Technological advancement has made it easy for individuals to log their personal information—including records of their physical location—to better use services that give them directions, local dinner recommendations, and other location-based services. Law enforcement has since caught on and begun seeking this location data to aid their investigations, using geofence warrants to identify individuals who use these location services and subpoenaing the technology companies that store the information.

This Note argues that the practice of geofencing violates an individual's reasonable expectation of privacy in their digital curtilage—a digital sphere of information that reflects intimate, private details of a person's life. This Note also proposes a reimagining of how geofence warrants could be altered to conform

* J.D., 2026, The George Washington University Law School; Honors B.A., 2017, University of Delaware. I am deeply grateful to the incredible editorial team of *The George Washington Law Review*, as well as my colleagues on the Senior Editorial Board, for their contributions in preparing this piece for publication. I am also sincerely thankful to Professor Carrie Montgomery for her invaluable feedback and guidance throughout the writing process. Additionally, I want to thank my family and friends for being there for me every step of the way. Finally, I dedicate this Note to my wife, Jess, whose unwavering support, constant encouragement, and gracious efforts to feign interest during countless discussions about geofences mean more than I can say.

with existing jurisprudence surrounding Fourth Amendment protections. This proposal recognizes the challenges posed by applying existing law to modern problems and balances privacy concerns with the need to keep pace with a continuously evolving technological world.

TABLE OF CONTENTS

INTRODUCTION	959
I. THE CURRENT LANDSCAPE OF THE GEOFENCE WARRANT	964
A. <i>Geofence Warrants and Their Use in Electronic Surveillance</i>	965
B. <i>The Development and Growth of Geofence Warrants</i>	967
C. <i>The Circuit Split</i>	968
II. EVOLVING ALONGSIDE TECHNOLOGY: BRINGING THE CONCEPT OF CURTILAGE TO A DIGITAL WORLD	972
A. <i>Location History Data Is a Form of Digital Curtilage Entitled to Fourth Amendment Protections</i>	973
B. <i>Intrusions Upon Digital Curtilage Account for More Significant Constitutional Violations</i>	976
III. INTRUDING ON DIGITAL CURTILAGE: THE PRIVACY FLAWS OF GEOFENCING	978
A. <i>Geofence Warrants Ignore Supreme Court Precedent</i>	978
B. <i>Geofence Warrants Must Meet Certain Requirements as Digital Curtilage Qualifies Outside Access of Location History Data as a Search</i>	981
IV. RECOGNIZING DIGITAL CURTILAGE AS A SOLUTION TO MODERN FOURTH AMENDMENT PRIVACY CONCERNS	983
A. <i>Adopting Digital Curtilage Is an Ideal Solution for Applying Fourth Amendment Jurisprudence in a Modern Society</i>	984
B. <i>The Practical Implications and Benefits of Adopting Digital Curtilage</i>	985
CONCLUSION	986

INTRODUCTION

“You had to live . . . in the assumption that every sound you made was overheard, and . . . every movement scrutinized.”¹ This quote from George Orwell’s *1984*, which was originally published in 1949,

¹ GEORGE ORWELL, 1984, at 6–7 (Signet Classics 2000) (1949).

has remained relevant in a world of constant technological innovation and growing privacy concerns. Though Orwell was keen enough to warn against dystopian hypermonitoring as early as the middle of the twentieth century, even he was likely unable to guess the capability that governments would one day have to oversee the activities of their populations.

In the seventy-five years since Orwell's novel hit the shelves, the world has seen drastic technological evolution, ranging from the creation of the internet to the invention of the cellphone and beyond. In 2025, ninety-eight percent of Americans owned a cellphone, and approximately nine out of ten of those cellphone-owning individuals owned smartphones.² This last figure is up from thirty-five percent found in a survey of smartphone ownership conducted in 2011.³

To utilize a number of features on their smartphones—like checking the weather forecast, finding local dinner recommendations, or using other location-based services—users must share their location with the relevant apps to get information tailored to their geographic region.⁴ The data these companies collect about a user's location does not always disappear after it has been used. Different companies use this information for various purposes: Some delete it for privacy reasons, and others sell it, use it for marketing or analysis, or share it with law enforcement.⁵

As of 2018, “[a]t least 75 companies receive[d] anonymous, precise location data from apps whose users enable location services” and “[s]everal of those businesses claim[ed] to track up to 200 million mobile devices in the United States—about half those in use [throughout 2017].”⁶ One of the most prominent companies that offers enhanced services to smartphone users who choose to share their location history data is ubiquitous in modern society: Google.

Google offers a number of applications and websites that provide additional services, like personalized recommendations, when users opt in to sharing their location information with the company, including

² See William Bishop et al., *Mobile Fact Sheet*, PEW RSCH. CTR. (Nov. 20, 2025), <https://www.pewresearch.org/internet/fact-sheet/mobile/> [https://perma.cc/K5VP-P3UW].

³ See *id.*

⁴ See Christopher Mims, *Your Location Data Is Being Sold—Often Without Your Knowledge*, WALL ST. J. (Mar. 4, 2018), <https://www.wsj.com/articles/your-location-data-is-being-soldoften-without-your-knowledge-1520168400> [https://perma.cc/9XLW-RBE2].

⁵ See Jennifer Valentino-DeVries, *How Your Phone Is Used to Track You, and What You Can Do About It*, N.Y. TIMES (Aug. 19, 2020), <https://www.nytimes.com/2020/08/19/technology/smartphone-location-tracking-opt-out.html> [https://perma.cc/77TV-6224].

⁶ Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller & Aaron Krolik, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), <https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html> [https://perma.cc/MF8J-FTQ5].

Google Maps, Chrome, Calendar, Drive, and Gmail.⁷ Additionally, Google's Android cellphones—which account for approximately seventy-four percent of smartphones globally—can track a device's location through the operating system, even when the user is not using a Google-created application.⁸ “Once a person enables Location History,” Google can track the user's location “across every *app* and every *device* associated with the user's account,” collecting location data approximately every two minutes, thereby maintaining a detailed account of a user's precise movements throughout the day.⁹

Traditionally, Google has stored users' location history data in Sensorvault, the company's location history database.¹⁰ Google has estimated that Sensorvault stores the location data from approximately 592 million different accounts worldwide.¹¹ This data is stored indefinitely and includes location records dating back to almost 2009.¹²

Due to its massive repository of location history data safely stored in one place, law enforcement agencies have sought Google's help in obtaining this data for various individuals of interest during criminal investigations.¹³ Specifically, law enforcement agencies have employed the use of a relatively new type of warrant, known as a geofence warrant, that targets specific geographic areas—called geofences—during specific timeframes.¹⁴ Geofence warrants are served on private companies to identify all devices that have passed within a geofence during the established period.¹⁵

Critics of geofence warrants often classify them as “reverse warrant[s],” or unconstitutional general warrants that lack probable cause and particularity because they collect device location data about every device falling within the warrant's parameters without identifying a

⁷ See *United States v. Chatrue*, 107 F.4th 319, 338 (4th Cir. 2024) (noting that once a user opts in to sharing location history with Google, the company “regularly obtains location data from your devices” and that the data is collected and saved “even when you aren't using a specific Google service, like Google Maps or Google Search”), *aff'd*, 136 F.4th 101 (4th Cir. 2025) (en banc) (per curiam), *vacated and remanded*, 146 S. Ct. 2193 (2026); see also Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2512 (2021) [hereinafter *Geofence Warrants and the Fourth Amendment*] (providing additional details about Google's technical capacity).

⁸ See *United States v. Smith*, 110 F.4th 817, 823 (5th Cir. 2024).

⁹ *Id.*

¹⁰ *Id.* at 822.

¹¹ *Id.* at 824.

¹² Jennifer Lynch, *Google's Sensorvault Can Tell Police Where You've Been*, ELEC. FRONTIER FOUND. (Apr. 18, 2019), <https://www.eff.org/deeplinks/2019/04/googles-sensorvault-can-tell-police-where-youve-been> [https://perma.cc/H9MK-36FY].

¹³ *Id.*

¹⁴ *Id.*

¹⁵ NAT'L ASS'N OF CRIM. DEF. LAWS., *GEOFENCE WARRANT PRIMER 1* (2023), https://www.nacdl.org/getattachment/816437c7-8943-425c-9b3b-4faf7da24bba/nacdl_geofence_warrant_primer_fourth_amendment_center_2023-08-29_v2.pdf [https://perma.cc/H4WH-XYMZ].

specific subject.¹⁶ Though Google has not been the only technology company to receive these warrants, it has received the overwhelming majority of geofence warrant requests.¹⁷ Google received its first geofence warrant in 2016, and since then, their use has increased dramatically.¹⁸ Additionally, they have become widely used by police departments throughout the United States.¹⁹

Geofence warrants have become controversial due to concerns not only over their sweeping intrusiveness but also because courts disagree over their constitutionality under the Fourth Amendment.²⁰ This controversy culminated in a circuit split between the Fourth and Fifth Circuits, which reached contrasting conclusions about whether these warrants are valid under the Fourth Amendment.²¹

The first point of divergence concerns whether accessing any amount of geofence records constitutes a search under the Fourth Amendment.²² The Fourth Circuit held that accessing such records is not a search if the “records sought are relatively limited in scale,” but the Fifth Circuit disagreed, classifying any access to this data by

¹⁶ *Id.*; *Smith*, 110 F.4th at 829.

¹⁷ Isha Marathe, *Tech Providers, Not Courts, May Have the Last Word on Geofence Warrants*, LAW.COM (Aug. 30, 2024, at 14:32 ET), <https://www.law.com/legaltechnews/2024/08/30/tech-providers-not-courts-may-have-the-last-word-on-geofence-warrants/> [https://perma.cc/766H-ZJ5S] (stating that in 2020, twenty-five percent of all warrants that Google received were geofence warrants, amounting to 11,554 different requests, with the number rising to nearly 35,000 by 2023).

¹⁸ *United States v. Chatrie*, 107 F.4th 319, 323 (4th Cir. 2024), *aff'd*, 136 F.4th 101 (4th Cir. 2025) (en banc) (per curiam), *vacated and remanded*, 146 S. Ct. 2193 (2026). In December 2023, Google announced that it would change the way that it handled user location information, which would limit the company’s ability to comply with geofence warrants in the future. For discussion surrounding this development, see *infra* Section I.B. See Skye Witley, *Google’s Location Data Move Will Reshape Geofence Warrant Use*, BLOOMBERG L. (Dec. 20, 2023, at 05:05 ET), <https://www.bloomberglaw.com/bloomberglawnews/privacy-and-data-security/X9ANDLH4000000> [https://perma.cc/PD9K-A3B3].

¹⁹ Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. TIMES (Apr. 13, 2019), <https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html> [https://perma.cc/UH28-ZQFE].

²⁰ See Ari Holtzblatt, George P. Varghese, Ericka Aiken & Whitney Russell, *The Impact and Future of the Fifth Circuit’s New Hard-Line Stance on Geofence Warrants*, WILMERHALE (Aug. 27, 2024), <https://www.wilmerhale.com/en/insights/client-alerts/20240827-the-impact-and-future-of-the-fifth-circuits-new-hard-line-stance-on-geofence-warrants> [https://perma.cc/D4RZ-YVVV].

²¹ *Compare Chatrie*, 107 F.4th at 319, with *Smith*, 110 F.4th at 817. Though these cases have recently garnered attention in the federal system, state courts previously considered some of the issues analyzed in these cases, including whether individuals maintain a reasonable expectation of privacy in the data collected by technology and data companies. See, e.g., *People v. Seymour*, 536 P.3d 1260, 1272 (Colo. 2023) (holding that the defendant had a reasonable expectation of privacy in his Google search history under the Colorado Constitution).

²² See Orin Kerr, *The Fifth Circuit Shuts Down Geofence Warrants—and Maybe a Lot More*, LAWFARE (Aug. 14, 2024, at 08:00 ET), <https://www.lawfaremedia.org/article/the-fifth-circuit-shuts-down-geofence-warrants-and-maybe-a-lot-more> [https://perma.cc/W9KE-RSSE].

law enforcement as a search.²³ In resolving part of this circuit split, the Supreme Court deemed such intrusions to be searches but has not reached a conclusion as to whether the searches are reasonable.²⁴ The second point of divergence concerns whether courts are ever permitted to issue a geofence warrant under the Fourth Amendment, given questions about whether such warrants can be sufficiently particularized when the database containing geofence records is so vast and must be searched in its entirety with each new warrant.²⁵ On this issue, the Fourth Circuit has upheld the validity of geofence warrants, but the Fifth Circuit has concluded that courts can never issue geofence warrants because they never comply with the Fourth Amendment.²⁶

This Note analyzes the threshold question at the heart of the circuit court split—whether law enforcement’s access to location history data constitutes a reasonable search under the Fourth Amendment. The scope of this Note will not expressly tackle geofence warrants’ complicity with the particularity requirement of the Fourth Amendment, though it will briefly discuss aspects regarding this issue in the context of the first question.

This Note argues that geofence warrants seek to access data to which individuals have a reasonable expectation of privacy and therefore result in unreasonable searches under the Fourth Amendment. These searches intrude upon an individual’s “digital curtilage”—the private digital sphere of information reflected in that person’s location history data.²⁷ A geofence warrant’s intrusion upon the digital curtilage ignores the particularity and individualized suspicion requirements of the Fourth Amendment. These warrants allow unreasonable searches of a person’s location history, which may reveal the most intimate details of a person’s life. This digital intrusion is analogous to intrusions upon physical curtilage—an area long protected under the Fourth Amendment. This Note proposes that the Supreme Court adopt the concept of digital curtilage to reshape the use of geofence warrants so that these

²³ *Id.*

²⁴ *Chatree v. United States*, 146 S. Ct. 2193, 2216–17 (2026).

²⁵ *See id.*

²⁶ *Id.*; *see Smith*, 110 F.4th at 817.

²⁷ The concept of digital curtilage was first proposed by Professor Andrew Ferguson in 2016 as a framework for extending Fourth Amendment protections to data stored locally on smart devices. *See* Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 867–72 (2016) (proposing a three-prong test for determining whether certain digital data should be protected as digital curtilage). Although Professor Ferguson’s framework provides a useful starting point for thinking about Fourth Amendment protections in a digital world, it does not contemplate the privacy concerns specific to geofencing—as the practice had not yet been widely adopted—nor does it account for nonlocal data that is collected, stored, and used by outside actors. This Note seeks to expand the concept of digital curtilage by including all private location history data that is intimately tied to the usage of everyday smart devices, regardless of where it is stored, in this data usage framework. *See infra* Section II.A.

warrants comply with the probable cause and particularity requirements governing Fourth Amendment searches.

Part I of this Note explains how geofence warrants are currently used and describes the current jurisprudence surrounding these warrants to illustrate their growing significance in modern law enforcement surveillance efforts. This Part also explores the implications of the split between the Fourth and Fifth Circuit Courts of Appeals, highlighting case law on what constitutes a search under the Fourth Amendment and whether that search is reasonable. Part II proposes the idea of recognizing location history data as digital curtilage, applying property doctrine adopted from Supreme Court precedent to the modern technological landscape. This comparison demonstrates that the location history data sought through geofence warrants is a new form of curtilage that should be afforded Fourth Amendment protection from unreasonable searches. Part III discusses how geofence warrants violate the Fourth Amendment's protections for digital curtilage. Lastly, Part IV argues that the Supreme Court should officially adopt the concept of digital curtilage to reframe how law enforcement may use geofence warrants while complying with existing Fourth Amendment jurisprudence.

I. THE CURRENT LANDSCAPE OF THE GEOFENCE WARRANT

Geofence warrants are primarily used in criminal investigations when law enforcement is unable to identify a suspect through traditional means, but these warrants have also been used to identify individuals in other situations.²⁸ For example, the most significant instance of geofence warrant requests used for the purpose of identifying large numbers of individuals occurred following the January 6, 2021 attack on the U.S. Capitol.²⁹ The Federal Bureau of Investigation pursued more geofence warrants than in any other single instance, identifying up to 5,723 devices “as being in or near” the Capitol “during the riot.”³⁰ Geofence warrants have become a versatile tool for law enforcement agencies, given that they are easy to pursue, inexpensive compared to traditional investigatory methods, and capable of revealing detailed information that can reflect both real-time and retroactive location history.³¹

²⁸ See NAT'L ASS'N OF CRIM. DEF. LAWS., *supra* note 15, at 1; *Geofence Warrants and the Fourth Amendment*, *supra* note 7, at 2513–14.

²⁹ Mark Harris, *A Peek Inside the FBI's Unprecedented January 6 Geofence Dragnet*, WIRED (Nov. 28, 2022, at 07:00 ET), <https://www.wired.com/story/fbi-google-geofence-warrant-january-6/> [<https://perma.cc/K9K7-6KPN>].

³⁰ This statistic is from a court filing from David Rhine, who was one of the suspects identified through the geofence warrants. *See id.*; *United States v. Rhine*, 652 F. Supp. 3d 38, 69 (D.D.C. 2023).

³¹ See *Geofence Warrants and the Fourth Amendment*, *supra* note 7, at 2510.

A. Geofence Warrants and Their Use in Electronic Surveillance

As with traditional warrants, law enforcement obtains geofence warrants through judicial approval, then serves them on a private company.³² All geofence warrants specify a search radius—the geofence—and a time frame, but the scope of each can vary significantly.³³ In fact, some geofence warrants will actually augment the search area by seeking devices “outside the search parameters but within a ‘margin of error.’”³⁴

As the largest recipient of geofence warrants, Google has “purported to ‘always push back on overly broad requests’” and, to that end, has developed a three-step procedure for handling these requests.³⁵ Much of the literature and jurisprudence surrounding geofence warrants references Google’s process, and this three-step procedure represents the most significant attempt by a company to respect individual privacy while still complying with geofence warrants.³⁶ This process has virtually become the standard for geofence warrant procedure.³⁷

First, because Google “has no way of knowing which accounts will produce responsive data, Google searches the entirety of Sensorvault,” which stores data from all 592 million different Google accounts, to produce anonymized results that satisfy the specifications of the geofence warrant.³⁸ Google then gives the anonymized results to law enforcement.³⁹ At this point, any results generally lead to law enforcement receiving an anonymous device identification number for each device within the geofence, but the data may also include “the date and time, the latitude and longitude, the geolocation source used, and the map display radius.”⁴⁰ When searching Sensorvault for this information, “Google does not impose specific, objective restraints on the size of the geofence, the length of the relevant timeframe, or the number of users

³² See *id.* at 2514.

³³ See *id.*

³⁴ *Id.* (quoting *In re Search of: Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 745 (N.D. Ill. 2020)).

³⁵ *Geofence Warrants and the Fourth Amendment*, *supra* note 7, at 2512–13, 2515.

³⁶ See *id.*; *United States v. Chatrie*, 107 F.4th 319, 324 (4th Cir. 2024), *aff’d*, 136 F.4th 101 (4th Cir. 2025) (en banc) (per curiam), *vacated and remanded*, 146 S. Ct. 2193 (2026); *United States v. Smith*, 110 F.4th 817, 824–26 (5th Cir. 2024); Orin S. Kerr, *The Fourth Amendment and Geofence Warrants: A Critical Look at United States v. Chatrie*, *LAWFARE* (Mar. 12, 2022), <https://www.lawfaremedia.org/article/fourth-amendment-and-geofence-warrants-critical-look-united-states-v-chatrie> [<https://perma.cc/TDY7-VG79>].

³⁷ See *Geofence Warrants and the Fourth Amendment*, *supra* note 7, at 2512–13, 2515.

³⁸ *Id.* at 2515; see *Smith*, 110 F.4th at 822–23.

³⁹ See NAT’L ASS’N OF CRIM. DEF. LAWS., *supra* note 15, at 1.

⁴⁰ *Smith*, 110 F.4th at 824–25.

for which [the geofence warrant] will produce data.”⁴¹ Instead, the company’s “Legal Investigation Specialist” reviews the warrant and “works with law enforcement to assuage any of Google’s concerns” before producing the results.⁴² Although this seems like a responsible measure by Google to safeguard user data, it does little to deter law enforcement agencies from making requests that violate this policy. For example, in *People v. Seymour*,⁴³ the Colorado Supreme Court detailed the Denver Police Department’s (“DPD”) attempts to serve a geofence warrant on Google.⁴⁴ In that case, the DPD failed to comply with Google’s policies twice and finally addressed the company’s concerns in its third warrant, which the DPD easily obtained despite having already failed to comply with the policies.⁴⁵

The second step requires law enforcement to review the anonymized information.⁴⁶ The government “culls [the information] using other investigative techniques” to identify devices of interest to the investigation.⁴⁷ At this step, law enforcement can request more information about specific accounts identified during step one—which may be done in a private letter without an additional warrant—and can seek “more location history for a longer period with no geographic limitations.”⁴⁸

In step three, the government requests identifying information for the devices flagged in the prior step.⁴⁹ This information can include, for example, the names, email addresses, and birthdates of the individuals associated with the devices. To receive the step-three identification information, the requestor is not required to provide any additional information, such as the investigative techniques used in step two or whether those techniques further connected the anonymized devices to the investigation.⁵⁰

41 *Id.* at 825 (quoting *United States v. Chatrie*, 590 F. Supp. 3d 901, 915 (E.D. Va. 2022), *aff’d*, 107 F.4th 319 (4th Cir. 2024), *aff’d*, 136 F.4th 101 (4th Cir. 2025) (en banc) (per curiam), *vacated and remanded*, 146 S. Ct. 2193 (2026)).

42 *Smith*, 110 F.4th at 825.

43 536 P.3d 1260 (Colo. 2023).

44 *Id.* at 1268–69.

45 *See id.* (describing how DPD violated Google’s policies with its first warrant by immediately seeking identifying information and with its second warrant by seeking two days of location data for a list of accounts instead of seeking personally identifying information of the relevant users).

46 *See Smith*, 110 F.4th at 825.

47 NAT’L ASS’N OF CRIM. DEF. LAWS., *supra* note 15, at 1.

48 *Id.*

49 *See id.*

50 *See United States v. Chatrie*, 107 F.4th 319, 350 n.4 (4th Cir. 2024) (Wynn, J., dissenting) (noting that Google has no established policy to determine when a request in step two has been appropriately investigated and the list of anonymized devices properly narrowed to request

B. *The Development and Growth of Geofence Warrants*

Although geofence warrants have surged since their initial use in 2016,⁵¹ their future remains uncertain.⁵² One source of uncertainty comes from the split between the Fourth and Fifth Circuits.⁵³ These circuits have reached different conclusions regarding whether obtaining data through a geofence warrant constitutes a search under the Fourth Amendment and whether those warrants are constitutional.⁵⁴ The Supreme Court has answered the first question in the affirmative, but leaves the second question unresolved.⁵⁵

A significant development affecting the future of geofence warrants comes from Google, which has changed how it stores location data.⁵⁶ In December of 2023, the company announced that it would limit its own access to user location data by encrypting the information and storing it locally on users' devices rather than in Sensorvault.⁵⁷ This change will effectively make it impossible for Google to comply with geofence warrant requests that seek information after the change is implemented, because Google will no longer have access to new location history data.⁵⁸ Although this will limit Google's ability to comply with geofence warrants going forward, the company will still be able to assist with requests for historical information because Sensorvault stores data indefinitely and includes records dating back to almost 2009.⁵⁹ Additionally, Google collects location data from users through methods other than location history, meaning that law enforcement agencies may still seek location information from Google through these alternative channels.⁶⁰

Although Google may not be able to comply with all geofence warrant requests in the future, these changes do not mean that geofence warrants will suddenly disappear. Given Google's prominence in receiving geofence warrants, it suddenly being unable to comply with this valuable investigative tool may result in law enforcement seeking to fill the vacuum left by Google's self-limitation. Law enforcement will likely

identification information), *aff'd*, 136 F.4th 101 (4th Cir. 2025) (en banc) (per curiam), *vacated and remanded*, 146 S. Ct. 2193 (2026).

⁵¹ See *supra* notes 17–18.

⁵² See *Chatrie*, 107 F.4th at 323–24.

⁵³ See *infra* Section I.C.

⁵⁴ See *infra* Section I.C.

⁵⁵ *Chatrie v. United States*, 146 S. Ct. 2193, 2216–17 (2026); see *infra* Section III.A.

⁵⁶ *Witley*, *supra* note 18.

⁵⁷ *Id.*

⁵⁸ *Id.*

⁵⁹ *Id.*

⁶⁰ Thomas Claburn, *Google Hopes to End Tsunami of Data Dragnet Warrants with Location History Shakeup*, THE REG. (Dec. 15, 2023, at 21:23 UTC), https://www.theregister.com/2023/12/15/google_location_history_geofence/ [<https://perma.cc/3XMT-57GQ>].

look to other third parties to fulfill their requests, many of which may not have the same level of protection in place as Google.⁶¹ There are many other technology companies with commonly used applications that track location data, including social media services like Facebook, Instagram, and Swarm.⁶²

In summary, even though Google appears to be stepping away from the world of geofence warrants, at least prospectively, there is an abundance of alternative players—including Lyft, Uber, Apple, and Snapchat, all of whom have already received geofence warrant requests—who can fill the void and are largely untested in this space.⁶³

C. *The Circuit Split*

The Fourth and Fifth Circuits split on geofencing and geofence warrant issues in July and August 2024, respectively.⁶⁴ The main question that the courts have grappled with is whether accessing a user's location history data constitutes a search under the Fourth Amendment.⁶⁵

The question of whether geofencing constitutes a search subject to the Fourth Amendment was first discussed in *United States v. Chatrie*.⁶⁶ In that case, the defendant, Okello T. Chatrie, became the subject of an investigation following a May 2019 bank robbery in Midlothian, Virginia.⁶⁷ The detective assigned to the robbery was unable to identify a suspect through traditional methods, so the detective sought a geofence

⁶¹ See Stephen Edelblut, *The End of the Beginning? Geofencing Warrants Face Backlash from 5th Circuit*, J. HIGH TECH. L.: BLOG (Jan. 8, 2025), <https://sites.suffolk.edu/jhtl/2025/01/08/the-end-of-the-beginning-geofencing-warrants-face-backlash-from-5th-circuit/> [https://perma.cc/BUV4-DJWX].

⁶² Cadie Thompson, *Social Media Apps Are Tracking Your Location in Shocking Detail*, BUS. INSIDER (May 28, 2015, at 18:25 ET), <https://www.businessinsider.com/three-ways-social-media-is-tracking-you-2015-5> [https://perma.cc/EFD2-SFCP].

⁶³ See Jackie O'Neil, *Much Ado About Geofence Warrants*, HARV. L. REV.: BLOG (Feb. 18, 2025), <https://harvardlawreview.org/blog/2025/02/much-ado-about-geofence-warrants/> [https://perma.cc/9XCR-GJLY].

⁶⁴ *Contrast* *United States v. Chatrie*, 107 F.4th 319 (4th Cir. 2024) (holding that a geofence warrant was not a Fourth Amendment search), *aff'd*, 136 F.4th 101 (4th Cir. 2025) (en banc) (per curiam), *vacated and remanded*, 146 S. Ct. 2193 (2026), *with* *United States v. Smith*, 110 F.4th 817 (5th Cir. 2024) (holding that a geofence warrant was a Fourth Amendment search). Notably, the Fourth Circuit granted rehearing en banc in *Chatrie* on November 1, 2024, but it ultimately affirmed the initial panel. *United States v. Chatrie*, 136 F.4th 100, 101 (4th Cir. 2025) (en banc) (per curiam), *vacated and remanded*, 146 S. Ct. 2193 (2026).

⁶⁵ See *supra* notes 20–26 and accompanying text.

⁶⁶ 107 F.4th 319 (4th Cir. 2024), *aff'd*, 136 F.4th 101 (4th Cir. 2025) (en banc) (per curiam), *vacated and remanded*, 146 S. Ct. 2193 (2026).

⁶⁷ *United States v. Chatrie*, 590 F. Supp. 3d 901, 905 (E.D. Va. 2022), *aff'd*, 107 F.4th 319 (4th Cir. 2024), *aff'd*, 136 F.4th 101 (4th Cir. 2025) (en banc) (per curiam), *vacated and remanded*, 146 S. Ct. 2193 (2026).

warrant.⁶⁸ The detective then proceeded through all three steps for obtaining data through a geofence warrant without any apparent method to narrow the anonymized data sought about the users from step one.⁶⁹ The deanonymized information that the detective ultimately received from step three “led the authorities to Chatrie,” resulting in his two-count indictment for the robbery.⁷⁰

Chatrie moved to suppress the evidence obtained from the geofence warrant.⁷¹ The district court concluded that the geofence warrant was invalid because it failed to satisfy the Fourth Amendment’s probable cause and particularity requirements for every user identified within the geofence.⁷² But the court nonetheless denied Chatrie’s motion to suppress under the good faith exception,⁷³ holding that because the detective “relied on the approval of prior [geofence] warrants in the face of novel technology,” his reliance on the warrant was not “objectively unreasonable.”⁷⁴ The court declined to address whether Chatrie had a reasonable expectation of privacy in his location data.⁷⁵

On appeal, the Fourth Circuit found that law enforcement’s acquisition of the defendant’s location history data did not constitute a search under the Fourth Amendment, so the geofence warrant used to obtain the data did not have to comply with the Amendment’s requirements.⁷⁶ The Fourth Circuit based its holding on two rationales. First, law enforcement did not obtain any personally revealing information about Chatrie because they only retrieved two hours of Chatrie’s location history data. Second, Chatrie opted in to using Google’s location services on his phone, which meant that the third-party doctrine applied, and thus Chatrie did not enjoy a reasonable expectation of

⁶⁸ *Chatrie*, 107 F.4th at 324.

⁶⁹ *Chatrie*, 590 F. Supp. 3d at 921. For information regarding the three steps for obtaining data via geofence warrants, see *supra* Section I.A.

⁷⁰ *Chatrie*, 590 F. Supp. 3d at 924. The step-three information is information that identifies the users associated with the specific accounts flagged by law enforcement officers during the previous steps. See *id.* at 916.

⁷¹ *Id.* at 925.

⁷² See *id.* at 927–35.

⁷³ See *United States v. Leon*, 468 U.S. 897, 900 (1984) (holding that the Fourth Amendment’s exclusionary rule, which allows for the suppression of information obtained from constitutionally invalid warrants, should not be applied to “evidence obtained by officers acting in reasonable reliance on a search warrant issued by a detached and neutral magistrate but ultimately found to be unsupported by probable cause”). The rule stemming from this holding is known as the good faith exception to the exclusionary rule.

⁷⁴ *Chatrie*, 590 F. Supp. 3d at 937–38.

⁷⁵ *Id.* at 925.

⁷⁶ *United States v. Chatrie*, 107 F.4th 319, 332 (4th Cir. 2024), *aff’d*, 136 F.4th 101 (4th Cir. 2025) (en banc) (per curiam), *vacated and remanded*, 146 S. Ct. 2193 (2026).

privacy in this data.⁷⁷ Under the third-party doctrine, individuals do not have a reasonable expectation of privacy in information they voluntarily disclose to a third party, even if that third party later relays it to government authorities.⁷⁸ The Fourth Circuit reaffirmed this holding when it reheard the case en banc in April 2025.⁷⁹

In *United States v. Smith*,⁸⁰ the Fifth Circuit disagreed with the Fourth Circuit's analysis and held that geofencing does constitute a Fourth Amendment search.⁸¹ *Smith* followed a similar fact pattern in which a robbery occurred, and police used a geofence warrant to identify a suspect.⁸² In order to return responsive information to comply with the subpoena from law enforcement, Google searched the entire Sensorvault—more than 592 million user accounts.⁸³ In attempting to identify a suspect, Google thus violated the privacy of every user with data in Sensorvault.⁸⁴

The Fifth Circuit reasoned that law enforcement conducts a search when seeking location history data and that individuals retain a reasonable expectation of privacy in that information—refuting both of the Fourth Circuit's rationales for reaching the opposite conclusion.⁸⁵ Addressing the Fourth Circuit's view that the data obtained could not be personally revealing because of the limited timeframe of the records requested, the Fifth Circuit stated that “the potential intrusiveness of even a snapshot of precise location data should not be understated.”⁸⁶ Even single moments can capture intimately personal information about a person's life or habits—“think a visit to ‘the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour-motel, the union meeting, the mosque, synagogue or church, [or] the gay bar.’”⁸⁷ Undoubtedly,

⁷⁷ *Id.* at 331. The third-party doctrine is a legal doctrine which maintains that “a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979). *But see* *Carpenter v. United States*, 585 U.S. 296, 309 (2017) (holding that the third-party doctrine does not apply to location history information of a person's physical movements as captured through cell-site location information because of the “unique nature of cell phone location records” as compared to other paradigmatic third-party information, such as physical business records).

⁷⁸ *See* *United States v. Miller*, 425 U.S. 435, 443 (1976).

⁷⁹ *See* *United States v. Chatrie*, 136 F.4th 101, 101 (4th Cir. 2025) (en banc) (per curiam), *vacated and remanded*, 146 S. Ct. 2193 (2026).

⁸⁰ 110 F.4th 817 (5th Cir. 2024).

⁸¹ *Id.* at 834.

⁸² *Id.* at 821.

⁸³ Holtzblatt et al., *supra* note 20.

⁸⁴ *See id.*

⁸⁵ *See Smith*, 110 F.4th at 832–36.

⁸⁶ *Id.* at 833.

⁸⁷ Haley Amster & Brett Diehl, *Against Geofences*, 74 STAN. L. REV. 385, 408 (2022) (alteration in original) (quoting *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

the intrusiveness of this data is why law enforcement has rapidly increased its efforts to obtain it; that location history data can easily uncover a person's "whole pattern of life," which gives law enforcement unprecedented insight into its suspects' habits and activities.⁸⁸ The Fifth Circuit highlighted that geofence location data "is invasive for Fourth Amendment purposes" and that this invasive nature stems from the "particular concern . . . that a geofence will retroactively track anyone with Location History enabled, regardless of whether a particular individual is suspicious or moving within an area that is typically granted Fourth Amendment protection."⁸⁹

In responding to the Fourth Circuit's conclusion that the third-party doctrine applies, the Fifth Circuit questioned whether users are truly informed when they opt in to location services and observed that the "notion that users voluntarily relinquish their right to privacy and 'assume the risk' of this information being divulged to law enforcement is dubious."⁹⁰ Even when individuals initially decline Google's location services, they are repeatedly prompted to opt in across multiple apps—often with promises of improved performance and with no warning that their location data will be indefinitely stored in Sensorvault.⁹¹ The Fifth Circuit also questioned whether the nature of the opt-in process is truly voluntary, given that more than 592 million people have "opted in" to the services.⁹² For these reasons, the court held that "law enforcement in this case *did* conduct a search when it sought Location History data from Google," underscoring the data's "intrusiveness and ubiquity."⁹³

Although the Supreme Court ultimately determined that accessing an individual's location history does constitute a search, the opinion has not resolved the debate as to whether using geofence warrants is reasonable under the Fourth Amendment.⁹⁴ Furthermore, the circuit split demonstrates a foundational disagreement between the two circuits regarding Fourth Amendment jurisprudence that may extend beyond the issue of geofencing. This Note suggests a clear, bright-line test to ensure consistent application of Fourth Amendment jurisprudence to modern disputes.

⁸⁸ Valentino-DeVries, *supra* note 19 (quoting Mark Bruley, Deputy Police Chief of Brooklyn Park, Minnesota).

⁸⁹ *See Smith*, 110 F.4th at 834.

⁹⁰ *Id.* at 835 (quoting *Smith v. Maryland*, 442 U.S. 735, 744 (1979)).

⁹¹ *See Smith*, 110 F.4th at 835.

⁹² *Id.* at 836.

⁹³ *Id.*

⁹⁴ *See supra* text accompanying notes 53–55.

II. EVOLVING ALONGSIDE TECHNOLOGY: BRINGING THE CONCEPT OF CURTILAGE TO A DIGITAL WORLD

The circuit split over the use of location history data demonstrates that existing jurisprudence concerning Fourth Amendment searches struggles to keep pace with technological searches in an evolving society. As courts diverge in their treatment of geofence warrants, the resulting patchwork of rules risks producing uneven constitutional protections across the country for the millions of people nationwide who have their location history data maintained.⁹⁵ This fragmentation gives rise to problems for both normal citizens and law enforcement agencies, including differing levels of privacy rights across jurisdictions and forum shopping.

The Supreme Court should adopt a standard framework that both addresses privacy concerns more broadly and clarifies the reasonable expectation of privacy in location history data. To do this, the Court should extend the property concept of curtilage to the modern context of location history data by recognizing it as a form of digital curtilage.

Curtilage is “the land immediately surrounding and associated with the home.”⁹⁶ The Supreme Court grants substantial privacy protections to the curtilage and considers it “*part of the home itself* for Fourth Amendment purposes.”⁹⁷ The Court has long relied on the concept of curtilage to extend Fourth Amendment protections “to the area immediately surrounding a dwelling house,” recognizing that a reasonable person “may expect” that the curtilage should be treated as part of the home.⁹⁸ Expanding this concept would modernize Fourth Amendment jurisprudence by allowing existing property doctrine to govern the classification of Fourth Amendment searches for location history data.

⁹⁵ See *Smith*, 110 F.4th at 824; see also *People v. Seymour*, 536 P.3d 1260, 1272 (Colo. 2023) (finding that geofence warrants are an illegal search under Colorado law).

⁹⁶ *Oliver v. United States*, 466 U.S. 170, 180 (1983) (emphasis added).

⁹⁷ *Id.*

⁹⁸ *United States v. Dunn*, 480 U.S. 294, 300–01 (1987) (holding that “defining the extent of a home’s curtilage” should be determined by analyzing “four factors: the proximity of the area claimed to be curtilage to the home, whether the area is included within an enclosure surrounding the home, the nature of the uses to which the area is put, and the steps taken by the resident to protect the area from observation by people passing by”); see *Collins v. Virginia*, 584 U.S. 586, 592 (2018); *California v. Ciraolo*, 476 U.S. 207, 212–13 (1986) (determining that the protection afforded to curtilage is an extension of the protection guaranteed to the home in “an area intimately linked to the home, both physically and psychologically, where privacy expectations are most heightened”).

A. *Location History Data Is a Form of Digital Curtilage Entitled to Fourth Amendment Protections*

Digital curtilage is a sphere of information generated by digital applications from a person's location history that reflects intimate, private details of a person's life.⁹⁹ Individuals should have a reasonable expectation of privacy in their digital curtilage because—much like physical curtilage—this information is “intimately linked” to their phones and portable electronic devices, which, like homes, require a warrant to search.¹⁰⁰

Analogizing digital curtilage to physical curtilage brings the concept into the modern age and protects the same underlying privacy interests. One way to understand physical curtilage is to consider the “area around the home to which the activity of home life extends.”¹⁰¹ This description applies to the concept of digital curtilage, recognizing that the location history logged by an electronic device is a natural extension of the device's activity.¹⁰² In defining physical curtilage, the Supreme Court identified the “central component” of the analysis as “whether the area harbors the ‘intimate activity associated with [an individual's home] and the privacies of life.’”¹⁰³ Although physical curtilage does not extend to activities too far removed from the home, this would not directly impair a digital curtilage analysis. This is because the “central component” of the curtilage test—the harboring of intimate activity—remains intact despite the lack of tangible data in the vicinity of the electronic device.

The Supreme Court has recognized that modern cellphones are entitled to Fourth Amendment protections and that they generally may not be searched without a warrant, absent exigent circumstances.¹⁰⁴ Under the definition of digital curtilage advanced above,¹⁰⁵ information gathered from a person's phone qualifies as protected digital curtilage because it could easily reveal “intimate activity” about numerous personal habits and associations.¹⁰⁶ In this sense, protecting digital curtilage from warrantless searches would reflect the same privacy interests as physical curtilage by protecting intimate and private information.

⁹⁹ See *supra* note 27 and accompanying text.

¹⁰⁰ *Ciraolo*, 476 U.S. at 212; see *Riley v. California*, 573 U.S. 373, 401–02 (2014) (holding that police officers could not search through the data of a cellphone without a warrant backed by probable cause, barring a reasonable exigent circumstance exception).

¹⁰¹ *Oliver*, 466 U.S. at 182 n.12.

¹⁰² See *id.*

¹⁰³ See *Dunn*, 480 U.S. at 300 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)); see also *Oliver*, 466 U.S. at 180 (quoting the same language from *Boyd*).

¹⁰⁴ See *Riley*, 573 U.S. at 402–03 (holding that modern cellphones hold “the privacies of life” and are “worthy of the protection for which the Founders fought”).

¹⁰⁵ See *supra* text accompanying note 100.

¹⁰⁶ See *Oliver*, 466 U.S. at 180; *United States v. Smith*, 110 F.4th 817, 833 (5th Cir. 2024).

Because of its parallels to physical curtilage, individuals should similarly have a reasonable expectation of privacy in their digital curtilage. One of the primary questions that courts face when they consider geofencing issues is whether obtaining geofence information constitutes a reasonable search under the Fourth Amendment.¹⁰⁷ This question is difficult to answer, and courts have not answered it consistently.¹⁰⁸ Under the third-party doctrine, generally, “a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.”¹⁰⁹

In *Carpenter v. United States*,¹¹⁰ the Supreme Court refused to extend the third-party doctrine to cell-site location information, which is a time-stamped record created whenever a cellphone connects to a cell tower while it continuously searches for the best possible signal.¹¹¹ The Court has emphasized that individuals “need to use a cell phone to participate in modern life . . . and you can’t opt out of creating cell site location records as they are automatically and necessarily created by using a cell phone.”¹¹²

Courts have since considered extending this concept to location history information, but there are some differences in determining whether that information is voluntarily shared by the user.¹¹³ The Fourth Circuit in *Chatrie* believed that no search was conducted under the third-party doctrine.¹¹⁴ The Fifth Circuit in *Smith*, however, reached the opposite conclusion, holding that a search was conducted when Smith’s location history information was requested and relying on *Carpenter* to conclude that the third-party doctrine did not apply.¹¹⁵ Specifically, the *Smith* court questioned the “voluntary” nature of opting in to use location services, stating that “a user simply cannot forfeit the protections of the Fourth Amendment for years of precise location information by selecting ‘YES, I’M IN’ at midnight while setting up Google Assistance, even if some text offered warning along the way.”¹¹⁶

Smith correctly concluded that the third-party doctrine does not apply to location history information, confirming that geofence warrants are Fourth Amendment searches in which individuals maintain

¹⁰⁷ See *United States v. Chatrie*, 107 F.4th 319, 325 (4th Cir. 2024), *aff’d*, 136 F.4th 101 (4th Cir. 2025) (en banc) (per curiam), *vacated and remanded*, 146 S. Ct. 2193 (2026); *Smith*, 110 F.4th at 830.

¹⁰⁸ See *Chatrie*, 107 F.4th at 332; *Smith*, 110 F.4th at 840.

¹⁰⁹ *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979).

¹¹⁰ 585 U.S. 296 (2018).

¹¹¹ See *id.* at 300.

¹¹² See Kerr, *supra* note 36.

¹¹³ Compare *Chatrie*, 107 F.4th at 332, with *Smith*, 110 F.4th at 836.

¹¹⁴ See *Chatrie*, 107 F.4th at 326–32.

¹¹⁵ See *Smith*, 110 F.4th at 836.

¹¹⁶ See *id.* (quoting *United States v. Chatrie*, 590 F. Supp. 3d 901, 936 (E.D. Va. 2022), *aff’d*, 107 F.4th 319 (4th Cir. 2024), *aff’d*, 136 F.4th 101 (4th Cir. 2025) (en banc) (per curiam), *vacated and remanded*, 146 S. Ct. 2193 (2026)); *supra* Section I.C.

a reasonable expectation of privacy. The third-party doctrine requires the relevant individual to consent to the sharing of their information. But “[a]s anyone with a smartphone can attest, electronic opt-in processes are hardly informed and, in many instances, may not even be voluntary.”¹¹⁷ Even when an individual initially declines to share their location data, repeated and opaque prompts often pressure users into eventually giving consent, regardless of whether they really intended to or whether they fully understands what their consent means.¹¹⁸ Moreover, it is

difficult to imagine that users of electronic devices would affirmatively realize . . . that they are providing their location information . . . in a way that will result in the government’s ability to obtain—easily, quickly and cheaply—their precise geographical location at virtually any point in the history of their use of the device.¹¹⁹

Given the absence of true informed consent, the third-party doctrine should not apply to an individual’s location history information.¹²⁰ The Supreme Court confirmed as much in its *Chatrie* opinion.¹²¹

Recognizing digital curtilage would offer a principled solution to the circuit split surrounding geofence warrants by eliminating the need for a third-party doctrine analysis. By recognizing digital curtilage as a protected extension of a cellphone’s use—much like how physical curtilage is where the life of the home extends—the information sought through a geofence warrant would be placed outside of the doctrine’s reach.¹²² Courts would instead ask whether the data sought reflects intimate activity that betrays the privacies of the individual’s life.¹²³ This approach allows courts to apply the same test used to determine whether a piece of property constitutes physical curtilage without requiring them to answer the subjective question of whether an individual voluntarily provided detailed information about his or her location to a

¹¹⁷ See *Smith*, 110 F.4th at 835 (citing Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1884–88 (2013)).

¹¹⁸ See *Smith*, 110 F.4th at 835–36.

¹¹⁹ *Id.* at 835 (quoting *In re Search of: Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 737 (N.D. Ill. 2020)).

¹²⁰ See *supra* text accompanying notes 105–13.

¹²¹ *Chatrie v. United States*, 146 S. Ct. 2193, 2213–15 (2026) (noting that the ordinary manner in which people use cell phones—by using the apps and services they provide—is “insulated from the third-party doctrine,” and does not constitute sharing private information with third parties).

¹²² See *id.*; see also *Oliver v. United States*, 466 U.S. 170, 182 n.12 (1984) (explaining how protections for the curtilage do not create a slippery slope problem for other aspects of Fourth Amendment jurisprudence, like the open fields doctrine).

¹²³ See *United States v. Dunn*, 480 U.S. 294, 300 (1987); *Oliver*, 466 U.S. at 180 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)).

third party.¹²⁴ Digital curtilage thus builds on and modernizes the precedent set in *Carpenter*, in which the Court held that voluntary exposure cannot truly exist when the relevant digital information is seen as “a pervasive and insistent part of daily life.”¹²⁵

B. Intrusions Upon Digital Curtilage Account for More Significant Constitutional Violations

Digital curtilage should be protected from warrantless intrusion by law enforcement because violations of digital curtilage via geofence warrants can result in even greater harms than traditional intrusions of physical curtilage. “[A] majority of the [Supreme] Court had ‘already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements,’” and multiple Justices have acknowledged that long-term Global Positioning System (“GPS”) monitoring infringes on reasonable expectations of privacy.¹²⁶

When law enforcement unlawfully intrudes upon physical curtilage, there is some sense that the damage can be contained. Suspects are typically aware of the intrusion because, when law enforcement enters their property, they can see what is happening in real time. In contrast, invasions of digital curtilage can occur in an essentially invisible manner, with the suspect never learning that the intrusion has occurred.¹²⁷ When law enforcement invades the physical curtilage, only the tangible items present at the location can be seen, seized, or otherwise used, and unlawfully obtained evidence can often be excluded in the event of legal action under the exclusionary rule.¹²⁸ But this remedy is not available for intrusions into an individual’s digital curtilage. These more advanced intrusions allow for “permeating police surveillance,” and geofences allow the government to achieve “near perfect surveillance” of an individual, given that carrying a cellphone “is essentially a prerequisite to participation in modern society.”¹²⁹

Unfettered access to this digital information can be more devastating to an individual because this “time-stamped data provides an

¹²⁴ See *Oliver*, 466 U.S. at 180; *Smith*, 110 F.4th at 835–36.

¹²⁵ *Carpenter v. United States*, 585 U.S. 296, 315 (2018) (quoting *Riley v. California*, 573 U.S. 373, 385 (2014)).

¹²⁶ *Smith*, 110 F.4th at 831 (quoting *Carpenter*, 585 U.S. at 310); see also *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (agreeing with Justice Samuel Alito’s stance that long-term GPS monitoring raises privacy concerns).

¹²⁷ See Elaine Silvestrini, *Your Smartphone May Get You Caught Up in a ‘Geofence Warrant,’* LEGAL EXAM’R (Sep. 23, 2025, at 06:26 ET), <https://www.legalexaminer.com/legal/your-smartphone-may-get-you-caught-up-in-a-geofence-warrant/> [https://perma.cc/3P74-MY2R].

¹²⁸ See *Mapp v. Ohio*, 367 U.S. 643, 655 (1961) (“[A]ll evidence obtained by searches and seizures in violation of the Constitution is, by that same authority, inadmissible in [federal and] state court.”).

¹²⁹ *Smith*, 110 F.4th at 833 (quoting *Carpenter*, 585 U.S. at 305, 311–12).

intimate window into a person's life."¹³⁰ Access to this variety of information betrays far more than just a person's physical location; it also provides an array of evidence that can be used to connect certain dots and illuminate intimate areas of a person's life that would be unknown through traditional investigative measures.¹³¹

Violations of digital curtilage also allow law enforcement to gain insight into private areas of a person's life that are wholly unrelated to the investigation, such as social activities, medical appointments, or other personal engagements. In *Carpenter*, the Court noted that the government acquired the defendant's cell-site location information pursuant to a court order issued under the Stored Communications Act,¹³² which "required the Government to show 'reasonable grounds' for believing that the records were 'relevant and material to an ongoing investigation.'"¹³³ This standard is a much lower showing than the probable cause required to obtain a warrant.¹³⁴ The Court, however, concluded that this threshold was unacceptably low for accessing information in which an individual has a reasonable expectation of privacy.¹³⁵ Without this determination, subpoenas of this nature could be used to circumvent the protections of the Fourth Amendment such that "no type of record would ever be protected by the warrant requirement."¹³⁶ This standard does not make it impossible for the government to obtain information within an individual's curtilage. Instead, the standard simply requires that a warrant—rather than a mere subpoena—be obtained when there is a legitimate privacy interest in the information sought.¹³⁷ Otherwise, subpoenas could be used "to acquire records in the overwhelming majority of investigations."¹³⁸

Geofencing poses a broad and potentially harmful risk resulting from such unrestricted data collection that is distinct from the traditional risks of physical intrusions. Geofence warrants can allow for indiscriminate

¹³⁰ *Carpenter*, 585 U.S. at 311.

¹³¹ See *Smith*, 110 F.4th at 831–34 (detailing how even limited location information accessed pursuant to a geofence warrant can follow an individual to several locations including medical establishments, places of worship, and attorney offices, which would likely not be uncovered through a mere physical search of an individual's property).

¹³² 18 U.S.C. §§ 2701–2713.

¹³³ *Carpenter*, 585 U.S. at 317; see also 18 U.S.C. § 2703(d) (permitting a court to order the disclosure of information governed by the Stored Communications Act only if the government can show that the information is relevant and material to an ongoing criminal investigation). As a result of the Court's decision in *Carpenter*, § 2703(d) orders are insufficient to obtain historical cell-site location information, though the statute remains operative for other disclosures under the Stored Communications Act. See *Carpenter*, 585 U.S. at 317.

¹³⁴ *Carpenter*, 585 U.S. at 317.

¹³⁵ See *id.*

¹³⁶ *Id.* at 318.

¹³⁷ See *id.*

¹³⁸ *Id.* at 319.

intrusion into the digital curtilage of numerous individuals who have no connection to an investigation but happened to pass through the geofence at the same time as a suspect.¹³⁹ Although several law enforcement officials have stated that the information collected from geofence warrants remains sealed in their states, this is not true in every state, which has led to public dissemination of the collected information.¹⁴⁰

III. INTRUDING ON DIGITAL CURTILAGE: THE PRIVACY FLAWS OF GEOFENCING

Though the Supreme Court has determined that accessing an individual's location history information constitutes a search, its opinion in *Chatrie* leaves many questions concerning Fourth Amendment jurisprudence unanswered.¹⁴¹ For example, the Supreme Court has not addressed whether geofence warrants comply with the probable cause and particularity requirements of the Fourth Amendment, which help to determine if a search is unreasonable and thus triggers Fourth Amendment protections.¹⁴²

A. *Geofence Warrants Ignore Supreme Court Precedent*

The Fourth Amendment of the U.S. Constitution guarantees individual privacy from unreasonable searches and seizures, providing in relevant part that

[t]he 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 . . . and particularly describing the place to be searched, and the persons or things to be seized.¹⁴³

In 1967, the Supreme Court heard a landmark case establishing new privacy standards, *Katz v. United States*.¹⁴⁴ In *Katz*, the Supreme Court introduced the “reasonable expectation of privacy” test for determining what constitutes a Fourth Amendment search, clarifying that the Fourth Amendment protects people—not places—from unreasonable searches and seizures.¹⁴⁵ The Court further stated that a search occurs

¹³⁹ See *Geofence Warrants and the Fourth Amendment*, *supra* note 7, at 2515.

¹⁴⁰ *Id.*

¹⁴¹ See *supra* text accompanying notes 53–55.

¹⁴² See *Chatrie v. United States*, 146 S. Ct. 2193, 2216–17 (2026) (holding that accessing an individual's location history is a search but declining to analyze whether the search in question was reasonable).

¹⁴³ U.S. CONST. amend. IV.

¹⁴⁴ 389 U.S. 347 (1967).

¹⁴⁵ See *id.* at 351; *United States v. Jones*, 565 U.S. 400, 405–06 (2012).

when a government action violates an individual's subjective expectation of privacy that society "is prepared to recognize as 'reasonable.'"¹⁴⁶

Applying the *Katz* test to digital curtilage weighs in favor of treating geofence warrants as Fourth Amendment searches.¹⁴⁷ Given the ubiquitous use of location data on cellphones and the general lack of informed consent regarding the sharing of this information, society would likely recognize an expectation of privacy in digital curtilage as reasonable.¹⁴⁸ Government attempts to obtain this information would therefore qualify as searches under the Fourth Amendment pursuant to the *Katz* test.¹⁴⁹

In 2012, the Supreme Court further developed its privacy jurisprudence in *United States v. Jones*,¹⁵⁰ a case that considered whether the duration of law enforcement monitoring bears on whether the monitoring constituted a search under the Fourth Amendment.¹⁵¹ Although the Court did not ultimately decide the question, concluding that it was unnecessary to make such a ruling in this case, it acknowledged that it may have to "grapple with these 'vexing problems'" in the future.¹⁵² In his concurrence, Justice Samuel Alito suggested that although the "relatively short-term monitoring of a person's movements . . . accords with expectations of privacy that our society has recognized as reasonable," longer-term GPS monitoring could infringe on these expectations of privacy.¹⁵³ Although this view does not constitute binding precedent, it can inform the analysis of treating digital curtilage intrusions as a Fourth Amendment search. Even though geofence warrants do not involve continuous monitoring, the government has access to a vast amount of location data that is not limited to a specific time.¹⁵⁴ The government can seek out location history information retroactively, gathering as much data as needed and effectively creating a long-term investigation in an instant with far less effort and fewer resources exhausted than would be required in a traditional investigation.¹⁵⁵

In 2018, the Supreme Court decided *Carpenter v. United States*,¹⁵⁶ which is the most analogous case to the issue of geofencing and digital

¹⁴⁶ *Katz*, 389 U.S. at 353, 361 (Harlan, J., concurring); see Orin S. Kerr, *Katz as Originalism*, 71 DUKE L.J. 1047, 1048 (2022).

¹⁴⁷ See *Katz*, 389 U.S. at 353; *Jones*, 565 U.S. at 405–06.

¹⁴⁸ See *supra* Section II.A.

¹⁴⁹ See *supra* Section II.A.; *Katz*, 389 U.S. at 350.

¹⁵⁰ 565 U.S. 400 (2012).

¹⁵¹ See *id.* at 412.

¹⁵² *Id.*

¹⁵³ *Jones*, 565 U.S. at 430 (Alito, J., concurring).

¹⁵⁴ See *Carpenter*, 585 U.S. at 311.

¹⁵⁵ *Id.*

¹⁵⁶ 585 U.S. 296 (2018).

curtilage.¹⁵⁷ In *Carpenter*, the Court acknowledged the privacy concerns surrounding digital location information data, holding that the acquisition of such information from cell sites constituted a Fourth Amendment search requiring a warrant.¹⁵⁸ This case builds on the considerations in *Jones*, holding that the cell-site location information sought here “presents even greater privacy concerns than . . . GPS monitoring.”¹⁵⁹

The concerns discussed in *Carpenter* reflect heavily on those present when discussing digital curtilage. The Court described how a cellphone “faithfully follows its owner beyond public thoroughfares and into private residences, doctor’s [sic] offices, political headquarters, and other potentially revealing locales.”¹⁶⁰ The Court also acknowledged that—like with geofencing—“the retrospective quality of the data . . . gives police access to a category of information otherwise unknowable,” allowing the government to recreate a person’s movements as far back as the information allows.¹⁶¹ The privacy concerns and details described in *Carpenter* are almost identical to those concerning geofencing and digital curtilage, with the only exception being that geofence warrants allow for an even greater intrusion into personally intimate information.¹⁶²

In 2026, the Supreme Court decided *Chatrie v. United States*.¹⁶³ Chatrie presented two questions to the Court to determine: (1) whether the execution of the geofence warrant in his case violated the Fourth Amendment, and (2) whether the exclusionary rule should apply to the evidence obtained pursuant to that warrant; however, the Court limited its analysis to the former question.¹⁶⁴

In this case, the Supreme Court determined definitively that government intrusion into a person’s location history as maintained by their smartphones and other electronic devices constitutes a search for Fourth Amendment purposes.¹⁶⁵ The Court, however, refused to make any other determinations, including whether the search was reasonable, whether the warrant satisfied Fourth Amendment requirements for probable cause and particularity, and how lower courts should determine whether geofence warrants comply with these requirements.¹⁶⁶ This case answered a major question—whether a geofence warrant is a

¹⁵⁷ See *id.* at 309–11.

¹⁵⁸ See *id.* at 316–20.

¹⁵⁹ *Id.* at 311.

¹⁶⁰ *Id.*

¹⁶¹ *Id.* at 312. At the time *Carpenter* was decided, wireless carriers’ retention policies maintained cell-site location information records for up to five years. *Id.*

¹⁶² *Id.* at 311.

¹⁶³ 146 S. Ct. 2193 (2026).

¹⁶⁴ *Chatrie*, 146 S. Ct. at 2203–04.

¹⁶⁵ *Id.*

¹⁶⁶ *Id.*; see *infra* Section III.B.

search—by clearly delineating that successfully serving a geofence warrant is a search for Fourth Amendment purposes.¹⁶⁷ The Supreme Court, however, left much to be determined in subsequent cases heard by lower courts, because it gave no clear test for whether or when geofence warrants comply with the probable cause and particularity requirements of the Fourth Amendment.

Geofence warrants currently allow law enforcement agencies to break with established Supreme Court precedent, permitting the government to intrude upon individuals' reasonable expectations of privacy to obtain intimate data for which a traditional warrant should be required.¹⁶⁸

B. Geofence Warrants Must Meet Certain Requirements as Digital Curtilage Qualifies Outside Access of Location History Data as a Search

In their current form, geofence warrants do not comply with Fourth Amendment jurisprudence. Their usage, however, can be reframed so that they can be an appropriate investigatory tool that conforms to the legal precedent governing Fourth Amendment searches.¹⁶⁹ There are several measures that law enforcement, the judiciary, and legislators could adopt to make geofencing more consistent with Fourth Amendment standards.

The absence of information identifying a suspect should not be sufficient to justify the issuance of a geofence warrant without additional “investigation-specific reasons to believe” that evidence leading to the specific suspect will be found within the warrant’s parameters.¹⁷⁰ Geofence warrants are primarily used to identify a suspect when no such information exists, and other investigative methods have failed.¹⁷¹ This practice ignores the Fourth Amendment’s particularity and probable cause requirements, instead constituting a “fishing expedition” in the hope that a suspect will be found by scraping data from an unknown number of random individuals.¹⁷² To combat this practice, law enforcement should be required to demonstrate particularity and

¹⁶⁷ *Chatrie*, 146 S. Ct. at 2203–04.

¹⁶⁸ See *supra* Section III.A.

¹⁶⁹ See *supra* Sections II.A, III.A.

¹⁷⁰ JENNIFER S. GRANICK, MAKING WARRANTS GREAT AGAIN 16 (2023), <https://www.aclu.org/wp-content/uploads/2023/05/Digital-Age-Warrants-May-2023-1.pdf> [<https://perma.cc/LH6W-JDDU>].

¹⁷¹ See *supra* Section I.A.

¹⁷² *United States v. Chatrice*, 107 F.4th 319, 353 (4th Cir. 2024) (Wynn, J., dissenting) (“[A geofence] warrant is uncomfortably akin to the sort of ‘reviled’ general warrants used by English authorities that the Framers intended the Fourth Amendment to forbid.” (quoting *Riley v. California*, 573 U.S. 373, 403 (2014))), *aff’d*, 136 F.4th 101 (4th Cir. 2025) (en banc) (per curiam), *vacated and remanded*, 146 S. Ct. 2193 (2026).

probable cause at each of the three stages used in obtaining data for a geofence warrant, clearly showing a connection between the geofence, the timeframe, and the potential suspect.¹⁷³ Failure to do so should not permit law enforcement to violate any individual's reasonable expectation of privacy in their digital curtilage.

The issues of particularity and probable cause are precisely where the Supreme Court's opinion in *Chatrie* does not extend far enough to determine whether the search was reasonable.¹⁷⁴ The Fourth Amendment protects individuals against *unreasonable* searches, not *all* searches.¹⁷⁵ Though the Supreme Court confirmed that law enforcement's access to Chatrie's location history information was indeed a search, it declined to answer whether the search was reasonable by analyzing whether the geofence warrant complied with the Fourth Amendment's particularity and probable cause requirements.¹⁷⁶ Instead, these questions were left to the Court of Appeals on remand.¹⁷⁷ This decision is dangerous because it leaves room for the appellate court to arrive at the same conclusion under the guise of different reasoning.

Some of the Justices were aware of this deficiency in the opinion. Justice Ketanji Brown Jackson's concurrence, joined by Justice Sonia Sotomayor, stated that she wrote separately from the opinion of the Court because she "would have gone further to explain that [the] search violated the Fourth Amendment."¹⁷⁸ Explaining further, Justice Jackson believed that, at a minimum, the second and third stages of law enforcement's search process did not satisfy the probable cause and particularity requirements.¹⁷⁹ She concluded by emphasizing the importance of these requirements and urged the Fourth Circuit to remember these requirements on remand.¹⁸⁰ Though the Court's opinion reaches the correct decision in deeming access to Chatrie's location history information a search, it leaves much to be desired by creating the space for the opinion to be virtually ignored with minimal effort.¹⁸¹

In addition to heightened standards for law enforcement, judicial involvement should be paramount throughout the geofence warrant

¹⁷³ See *supra* Section I.A.

¹⁷⁴ See *Chatrie v. United States*, 146 S. Ct. 2193, 2216–17 (2026) (declining to address the question as to whether law enforcement satisfied the probable cause and particularity requirements at each step of the process to obtain the geofence warrant and leaving the matter to the Fourth Circuit).

¹⁷⁵ U.S. CONST. amend. IV.

¹⁷⁶ See *Chatrie*, 146 S. Ct. at 2216–17.

¹⁷⁷ See *id.*

¹⁷⁸ *Id.* at 2217 (Jackson, J., concurring).

¹⁷⁹ *Id.*

¹⁸⁰ *Id.* at 2218.

¹⁸¹ See *id.* at 2216–17 (majority opinion) (allowing the Fourth Circuit to make a new determination on the admissibility of the evidence without explicitly requiring a constitutional analysis of adherence to the Fourth Amendment at each step of law enforcement's search).

process. Currently, a judge is only required to sign off on the geofence warrant used to obtain the anonymized data in step one of the geofence procedure; there is no judicial oversight governing steps two and three concerning the investigation and identification of the data provided in step one.¹⁸² Requiring judicial approval using Fourth Amendment warrant standards at each step of the geofence process would safeguard digital curtilage by ensuring that law enforcement meets constitutional privacy protections while still investigating effectively.¹⁸³ To enforce this, law enforcement officers should be required to obtain judicial approval at each step, in light of any new investigatory methods used or information obtained since receiving approval at the previous step in the process. This requirement would also serve a secondary purpose: strengthening the good faith exception to the exclusionary rule, because good faith would presumably be more easily found in cases in which a warrant has properly survived judicial scrutiny on three separate occasions.¹⁸⁴

Beyond more stringent standards for data collection, there must also be clear rules concerning the retention of any information collected through a geofence warrant. Although judges often seal these warrants, this practice is not required, and the information obtained through geofence warrants does not always remain sealed in every state.¹⁸⁵ Federal legislators should pass laws establishing privacy protections for geofence warrants, including proper sealing of the warrants and the information obtained, as well as the appropriate deletion of information that is not ultimately useful to the investigation.¹⁸⁶

These guidelines would not prohibit the use of geofence warrants, but they would establish accountability for the law enforcement agencies that have essentially had *carte blanche* to use them without constraints. These suggestions would allow for the continued use of geofence warrants, but in a manner that better balances investigatory needs with the privacy rights protected by the Fourth Amendment.¹⁸⁷

IV. RECOGNIZING DIGITAL CURTILAGE AS A SOLUTION TO MODERN FOURTH AMENDMENT PRIVACY CONCERNS

Digital curtilage can help bridge the gap between existing laws and technological innovation by providing a framework to consider new information under a familiar light. This concept can help apply existing

¹⁸² See *supra* Section I.A.

¹⁸³ See *supra* Section I.A.

¹⁸⁴ *Chatrle*, 146 S. Ct. at 2216 (“It is therefore now up to the Court of Appeals to decide whether, *at each step of the search process*, the warrant satisfied the Fourth Amendment’s requirements of particularity and probable cause.”) (emphasis added).

¹⁸⁵ Valentino-DeVries, *supra* note 19.

¹⁸⁶ See *supra* Section I.A.

¹⁸⁷ See *supra* Section I.A.

legal principles to unfamiliar territory while also addressing future privacy concerns.¹⁸⁸

A. *Adopting Digital Curtilage Is an Ideal Solution for Applying Fourth Amendment Jurisprudence in a Modern Society*

Digital curtilage is a logical extension of the existing physical curtilage doctrine that aligns with recent precedent governing new investigatory techniques.¹⁸⁹ Digital curtilage should be treated like physical curtilage, which would take technology usage—a fundamental aspect of daily living—and extend privacy protections to the intimate activity created by essential technological tools used by hundreds of millions of individuals.¹⁹⁰

Beyond serving as an analog to physical curtilage, digital curtilage extends the principles established by decades of legal precedent to the digital world. Digital curtilage captures the reasonable expectation of privacy concept and test from *Katz*, establishing location information as a societally accepted source of personal information.¹⁹¹ Furthermore, the concept of digital curtilage reflects *Jones*'s concern with the duration of location tracking and *Carpenter*'s recognition that individuals retain a reasonable expectation of privacy in cell-site location information. By imposing limits on law enforcement's potentially unlimited reach into an individual's historical location data, digital curtilage gives effect to the principles articulated in these Supreme Court decisions.¹⁹²

In addition to embodying the jurisprudence surrounding Fourth Amendment privacy protections, digital curtilage offers flexibility by allowing law enforcement to continue using geofence warrants to comply with those protections.¹⁹³ Digital curtilage establishes a clear test for determining what constitutes a Fourth Amendment search: digital information that reflects private details of an individual's life and is intimately linked to their phones and other devices.¹⁹⁴ Furthermore, it provides a sense of what constitutes a reasonable search by analogizing digital curtilage to the long-established concept of physical curtilage, which requires the same level of constitutional protection.¹⁹⁵ This clarity gives law enforcement predictable boundaries within which they can

¹⁸⁸ See *infra* Section IV.B.

¹⁸⁹ See *supra* Sections I.A., II.A., III.A.

¹⁹⁰ See *supra* Section II.A.

¹⁹¹ See *supra* Section II.A.

¹⁹² See *supra* Section II.A.

¹⁹³ See *supra* Section III.B.

¹⁹⁴ See *supra* Section I.A.

¹⁹⁵ See *supra* Section II.A.

work, balancing law enforcement's needs with the privacy interests of modern society.¹⁹⁶

B. The Practical Implications and Benefits of Adopting Digital Curtilage

Although digital curtilage seems to fit well within the privacy protections in current Fourth Amendment jurisprudence, there are bound to be some who raise concerns regarding the adaptation of an existing doctrine of law to fit newer problems. For example, the Fourth Circuit appears to disagree with the premise that location history data always provides “an intimate window into [a person’s] life.”¹⁹⁷ The court did not believe that a record of a “single, brief trip” violated a reasonable expectation of privacy given that the information is “less revealing than [the information] obtained in *Jones* [or] *Carpenter*.”¹⁹⁸ This opinion, however, does not seem to fully appreciate what even a “single, brief trip” can betray.¹⁹⁹ One data point is sufficient to reveal deeply personal details and expose the rhythms of someone’s private life.²⁰⁰

Digital curtilage also serves as a flexible measure to safeguard privacy while enabling law enforcement to investigate as they see fit. The digital curtilage concept does not prohibit the use of any investigative methods, namely geofence warrants; rather, it establishes concrete and predictable guidance regarding their use, enabling law enforcement to keep using this valuable tool without fear of having any resulting evidence excluded at trial.²⁰¹ This serves to balance the interests of law enforcement efforts with evolving privacy concerns, enabling both groups to evolve alongside one another.

Though there are potential critiques regarding the adoption of digital curtilage as a privacy framework for future Fourth Amendment search questions, the practical benefits resulting from doing so would be substantial. First, and most notably, privacy protections would be properly

¹⁹⁶ See *supra* Section I.A.

¹⁹⁷ *United States v. Chatrie*, 107 F.4th 319, 330 (4th Cir. 2024) (explaining that the geofence data obtained by the government could not provide an “intimate window” into the defendant’s personal life given that only two hours’ worth of data were obtained and that the government could not deduce information about the defendant’s life with only an “individual trip viewed in isolation”), *aff’d*, 136 F.4th 101 (4th Cir. 2025) (en banc) (per curiam), *vacated and remanded*, 146 S. Ct. 2193 (2026).

¹⁹⁸ *Id.* at 330–31.

¹⁹⁹ See *United States v. Smith*, 110 F.4th 817, 833–34 (5th Cir. 2024) (explaining that the “potential intrusiveness of even a snapshot of precise location data should not be understated” because such information can allow an unknown observer to glean intimate insight into a person’s private life).

²⁰⁰ *Id.*; see *Amster & Diehl, supra* note 87, at 408 (quoting *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

²⁰¹ See *supra* Sections II.A, III.A.

accounted for in Fourth Amendment search situations.²⁰² Digital curtilage's focus on protecting the highly sensitive data of numerous innocent individuals would solidify the intentions behind the Fourth Amendment, allowing the legal framework to catch up with modern times.²⁰³

Finally, digital curtilage will effectively establish a pathway for Fourth Amendment jurisprudence to adapt to future advancements so that similar concerns and confusion do not arise as technology continues to evolve at a pace that outstrips societal imagination. Digital curtilage is not tied directly to a specific technology or investigative method.²⁰⁴ Instead, the doctrine adapts a traditional legal framework to address a gap created by technological innovation that puts personal data at risk through the use of fundamental and necessary technologies.²⁰⁵ Framing digital curtilage in this way allows the concept to be used easily to address future privacy concerns stemming from further technological development, whether from artificial intelligence, new forms of mass surveillance, or a currently unimagined technology.²⁰⁶ Digital curtilage is a malleable legal concept that will provide balance in the Fourth Amendment doctrine. Its flexibility is the foundation of a useful framework for both citizens and law enforcement, even as technology rapidly advances.

CONCLUSION

Rapid technological advancement has created new and previously unimaginable privacy concerns for society that were not considered when the fundamental rights and laws governing privacy protection were first established. This has left a gap in the jurisprudence outlining Fourth Amendment protections concerning the unconstitutional search of digital information that reveals the intimate details of individuals throughout society.

The concept of digital curtilage can be adopted to bridge the gap between the existing law and new privacy concerns. Digital curtilage provides a flexible framework that permits the collection of this data under appropriate conditions, matching the privacy protections already in place for physical intrusions by law enforcement under established privacy requirements. Digital curtilage provides a path forward, easily allowing for the continued development of technology while adapting to ensure that privacy considerations are protected in the future.

²⁰² See *supra* Section II.A.

²⁰³ See *supra* Section II.A.

²⁰⁴ See *supra* Section II.A.

²⁰⁵ See *supra* Section II.A.

²⁰⁶ See *supra* Section II.A.