The Post-Dobbs Reality: Privacy Expectations for Period-Tracking Apps in Criminal Abortion Prosecutions

Sophie L. Nelson

Follow this and additional works at: https://digitalcommons.pepperdine.edu/plr

Part of the Constitutional Law Commons, Fourth Amendment Commons, Privacy Law Commons, and the Science and Technology Law Commons

Recommended Citation
Available at: https://digitalcommons.pepperdine.edu/plr/vol51/iss4/3

This Comment is brought to you for free and open access by the Caruso School of Law at Pepperdine Digital Commons. It has been accepted for inclusion in Pepperdine Law Review by an authorized editor of Pepperdine Digital Commons. For more information, please contact bailey.berry@pepperdine.edu.
The Post-Dobbs Reality:

Privacy Expectations for Period-Tracking Apps in Criminal Abortion Prosecutions

ABSTRACT

The Supreme Court’s decision to overturn Roe v. Wade and Planned Parenthood v. Casey in June 2022 was met with waves of both support and criticism throughout the United States. Several states immediately implemented or began drafting trigger laws that criminalize seeking and providing an abortion. These laws prompted several period-tracking app companies to encrypt their users’ data to make it more difficult for the government to access period- and pregnancy-related information for criminal investigations. This Comment explores whether the Fourth Amendment and U.S. privacy statutes protect users of period-tracking apps from government surveillance. More specifically, this Comment argues that the Supreme Court’s holding in Carpenter v. United States—that an individual has a reasonable expectation of privacy in their cell-site location information—should extend to personal information placed in period-tracking apps. This Comment also urges Congress to adopt a comprehensive federal privacy statute to address the gaps in consumer privacy protections currently in force at the federal and state levels. Our courts and government should recognize that the pervasive and comprehensive wealth of personal information on our cell phones deserves protection from government interference, especially when such information reveals the health and sexual intimacies of millions of women across the United States.
# TABLE OF CONTENTS

I. **INTRODUCTION** ........................................................................................................ 785

II. **THE FOURTH AMENDMENT: WHAT IS A REASONABLE EXPECTATION OF PRIVACY?** ....................................................................................................................... 788
   A. The Foundation ........................................................................................................ 788
   B. The Fourth Amendment Adapts to Modern Surveillance Technology .................. 790
   C. The Third-Party Doctrine’s Extra Layer ................................................................. 791

III. **CURRENT STATE OF THE LAW: THE CARPENTER FRAMEWORK AND AMERICAN PRIVACY STATUTES** .................................................................................. 793
   A. The Technological Exceptionalism Recognized by Carpenter .............................. 793
   B. The Carpenter Framework ...................................................................................... 794
   C. Praise and Criticism for Carpenter ....................................................................... 796
   D. Current Federal and State Privacy Statutes ......................................................... 797

IV. **PRIVACY AND PERIOD-TRACKING APPS IN A POST-DOBBS NATION** ............. 802
   A. Encryption and Period-Tracking Apps .................................................................. 805
   B. The Third-Party Doctrine and Encrypted Period-Tracking Apps ......................... 806
   C. Federal and State Privacy Statutory Protections over Period-Tracking Apps ........ 810

V. **IMPACT AND SIGNIFICANCE: RECONCILING CARPENTER AND THE PRIVACY OF APP DATA** ................................................................................................. 813
   A. What Would the Current Supreme Court Think? ............................................... 813
   B. A Call to Action for Congress to Codify National Privacy Legislation ................ 815
   C. Impacts and Consequences for Users of Period-Tracking Apps ........................ 816

VI. **CONCLUSION** .......................................................................................................... 818
I. INTRODUCTION

“Pregnant? Don’t Want to Be? Call NO ONE.”¹

The Supreme Court’s decision to overturn Roe v. Wade and Planned Parenthood v. Casey in June 2022 elicited drastically different reactions across the nation, with some celebrating the preservation of fetal life and others mourning the loss of women’s reproductive autonomy.² At the time of the Court’s decision, thirteen state legislatures already had “trigger laws” that were “written to automatically go into effect following the overturning of Roe v. Wade.”³ These bans make obtaining or providing an abortion susceptible to criminal prosecution, and many states do not provide exceptions for rape or incest.⁴

In response to Dobbs and the trigger laws, several period-tracking app companies assured users that they would use data encryption to protect users’ private reproductive health information from government surveillance.⁵ Nevertheless, women⁶ in these trigger-law states immediately began preparing for

4. Id. The trigger laws in Kentucky, Louisiana, Missouri, North Dakota, Oklahoma, South Dakota, Tennessee, and Texas do not provide such exceptions. Id.
5. See Lucas Ropek, Should You Use This Encrypted Period Tracking App?, GIZMODO (June 28, 2022), https://gizmodo.com/stardust-roev-wade-encrypted-period-tracking-app-abort-1849113572. Data encryption converts text and data “from a readable format into an encoded format” that “can only be read or processed after it’s been decrypted” by a key. What is Data Encryption?, KASPERSKY, https://usa.kaspersky.com/resource-center/definitions/encryption (last visited Jan. 14, 2024); see also infra Section IV.A.
6. I recognize the now-common preference for using the terminology “pregnant people” in place of “women” in the context of abortion debate and policy. See Carrie N. Baker & Carly Thomsen, The Importance of Talking About Women in the Fight Against Abortion Bans, MS. MAG. (June 23, 2022), https://msmagazine.com/2022/06/23/women-abortion-bans-inclusive-language-pregnant-people/. I also recognize that many advocates do not employ the term “pregnant people” because using sex-neutral language “risks obscuring the sexism underlying anti-abortion laws and policies” that
a post-*Dobbs* reality by deleting their fertility and period-tracking apps out of fear that the government could use their data in a criminal abortion prosecution.⁷

Furthermore, legal scholars have expressed concern about government access to sensitive data because of the ubiquitous role of technology and data-sharing in our everyday lives.⁸ For example, Professor Jennifer Lauren expressed her concerns that “from an evidentiary standpoint, [she] can see how the [period-tracking app] information would be valuable” to the government in criminal prosecutions.⁹ Digital information like purchasing history, internet search history, and encrypted data entered into period-tracking apps may be susceptible to government subpoena for use in a criminal prosecution without the need for a warrant or probable cause.¹⁰ Even smartphone apps that do not use GPS-tracking data sell users’ personal data and location information to third parties, raising reasonable concerns about the efficacy of privacy protections implemented by smartphone app companies.¹¹

The intimate and advanced nature of technology today deeply contrasts historically targeted women. *Id.* Throughout this Comment, I use the term “women,” but I recognize that abortion decisions may also affect many nonbinary and transgender individuals who are at risk of getting pregnant.

¹⁷ Evan MacDonald, *After Roe v. Wade Ruling, Houston Women Are Deleting Period Tracking Apps, Citing Privacy Concerns*, HOUS. CHRON., https://www.houstonchronicle.com/lifestyle/renew-houston/health/article/Period-tracking-apps-spark-panic-after-Roe-v-17279151.php (last updated July 5, 2022, 11:59 AM); see also Mackenzie K. Mendolla, Comment, *A Blurry Lens: Assessing the Complicated Legal Landscape of Biometric Privacy Through the Perspective of Mobile Apps*, 54 SETON HALL L. REV. 923, 929 (2024) (“Following *Dobbs*, there has been increased concern over the ways in which private companies collect sensitive health information without proper privacy protections in place. Most notably, concern has increased over law enforcement’s ability to access the data that these companies collect.”).

¹⁸ See, e.g., Cynthia Conti-Cook, *Surveilling the Digital Abortion Diary*, 50 U. BALTIMORE L. REV. 1, 51–56 (2020) (discussing several avenues that the government can take to find a digital trail of evidence in a criminal abortion prosecution).

¹⁹ MacDonald, *supra* note 7.


with that used by pre-Roe women who sought abortions. Before Roe, a cohort of activists formed an underground organization in Chicago called the “Jane Collective” (the Janes) that provided illegal abortions to women who were unable to obtain one. The Janes targeted their services through simple newspaper advertisements that stated: “Pregnant? Don’t Want to Be? Call Jane.”

Although the Janes flew under the radar for several years in the 1960s and 1970s, a similar operation would immediately be tracked and dismantled today by way of technological advancements. For example, “location history is available both through digital device extractions and subpoenas,” which law enforcement can easily obtain to determine the possible location of an underground abortion clinic. Additionally, the government could use social media activity, internet search history, and data from wearable devices—such as Apple Watches and Fitbits—to gather evidence about the whereabouts of people seeking abortions and the locations of those clinics.

The Fourth Amendment fundamentally protects Americans from government searches when the party subject to a search has a “reasonable expectation of privacy.” The third-party doctrine generally allows the government to collect information that an individual voluntarily shares with third parties. However, in 2018, the Supreme Court held in Carpenter v. United States that an individual has a legitimate expectation of privacy in cell-site location information collected by cell phone carriers, concluding that not all information is truly “voluntarily” shared with third-party companies. Furthermore, the lack of a comprehensive federal privacy statute allows app companies and the government to easily access sensitive personal data, largely leaving the onus

12. See Haberman, supra note 1 (contrasting pre-Roe abortion methods from those now possible post-Dobbs).
15. See, e.g., Conti-Cook, supra note 8, at 51–56 (identifying different types of digital resources law enforcement can use to build a case against pregnant women).
16. Id. at 51.
17. See id. at 54–55, 73.
19. See Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (“This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.”); see also United States v. Miller, 425 U.S. 435, 443 (1976).
on states to protect private information.\textsuperscript{21}

This Comment analyzes these different aspects of Fourth Amendment and privacy law by specifically discussing whether data voluntarily logged into period-tracking apps can be accessed by the government without a warrant in criminal abortion investigations.\textsuperscript{22} Part II reviews the history and development of Fourth Amendment law.\textsuperscript{23} Part III discusses the state of Carpenter as applied to the current technological age, in addition to the federal privacy scheme and how some states, particularly California, have taken data privacy legislation into their own hands.\textsuperscript{24} Part IV applies Carpenter and other privacy statutes to period-tracking apps and concludes that Carpenter may provide a useful framework in future privacy litigation but that current American privacy statutes do not adequately protect app users’ data.\textsuperscript{25} Part V analyzes the impact and significance of this area of law, focusing on whether the current Supreme Court would extend Carpenter to all types of cell phone data and providing a call to action for Congress to pass a federal statute that protects this data from warrantless government seizures.\textsuperscript{26} Finally, Part VI concludes with a summary of the law and why the government must urgently act to protect the personal data of millions of Americans who face the risk government overreach in accessing their intimate information.\textsuperscript{27}

II. THE FOURTH AMENDMENT: WHAT IS A REASONABLE EXPECTATION OF PRIVACY?

A. The Foundation

The Fourth Amendment guarantees “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.”\textsuperscript{28} It generally requires the government to have probable cause and/or a warrant before conducting a search or seizure of an individual’s items

\begin{itemize}
  \item \textsuperscript{22} \textit{See infra} Parts II–VI.
  \item \textsuperscript{23} \textit{See infra} Part II.
  \item \textsuperscript{24} \textit{See infra} Part III.
  \item \textsuperscript{25} \textit{See infra} Part IV.
  \item \textsuperscript{26} \textit{See infra} Part V.
  \item \textsuperscript{27} \textit{See infra} Part VI.
  \item \textsuperscript{28} U.S. CONST. amend. IV.
\end{itemize}
The Fourth Amendment “was first established to prevent a powerful government from issuing broad sweeping general warrants,” which England had administered during colonial times to help enforce British mandates. Until the mid-twentieth century, the Supreme Court interpreted the Fourth Amendment to primarily protect individuals’ real property interests from unreasonable government invasions.

In the 1960s, the Supreme Court in *Katz v. United States* expanded Fourth Amendment protections and laid the foundation for the United States’ modern Fourth Amendment jurisprudence. There, the FBI suspected Charles Katz of transmitting wagering information in violation of federal law. To investigate further, the agents attached an electronic recording device to the outside of a public telephone booth, through which they heard incriminating evidence that resulted in Katz’s conviction. Although prior Supreme Court precedent predominately applied the Fourth Amendment to physical intrusions onto private property, for the first time the Court recognized that “the Fourth Amendment protects people, not places.”

From this declaration, the Court established the “reasonable expectation of privacy” test, under which an unconstitutional Fourth Amendment search occurs when the person being searched exhibits a subjective expectation of privacy and their expectation is one that society is objectively prepared to

30. Marisa Kay, *Reviving the Fourth Amendment: Reasonable Expectation of Privacy in a Cell Phone Age*, 50 J. MARSHALL L. REV. 555, 559 & n.30 (2017). In colonial times, British customs officers imposed general warrants to search and seize goods on which American colonists did not pay taxes. Silas J. Wasserstrom & Louis Michael Seidman, *The Fourth Amendment as Constitutional Theory*, 77 GEO. L.J. 19, 54–55 n.142 (1988). These warrants did not require probable cause or specificity as to the places to search or items to seize. *Id.* Thus, when the Founding generation ratified the Fourth Amendment, they intended for it to act as a check on police power by requiring probable cause and specificity before conducting searches and seizures. *Id.*; *see also* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890) (recognizing over 130 years ago that “in very early times, the law gave a remedy only for physical interference with life and property” and highlighting that “[p]olitical, social, and economic changes entail the recognition of new rights, and the common law . . . grows to meet the demands of society.”).
31. Kay, *supra* note 30, at 559 (“[T]he Supreme Court initially interpreted the Fourth Amendment as protecting individuals from unreasonable physical intrusion upon individuals’ real property.”).
33. *Id.* at 348.
34. *Id.*
recognize as reasonable. The Supreme Court has not “specifically declared which privacy expectations are entitled to protection but instead has relied on guiding principles.” Nevertheless, this test “is the foundation of modern Fourth Amendment jurisprudence” and provides protection against unwarranted law enforcement surveillance, even absent a physical intrusion.

B. The Fourth Amendment Adapts to Modern Surveillance Technology

Perhaps unsurprisingly, modern police surveillance technology has vastly developed and expanded since the Supreme Court decided Katz in 1967. The Supreme Court significantly expanded its Fourth Amendment jurisprudence in Kyllo v. United States to keep up with ever-changing surveillance technology. There, law enforcement used a thermal imaging device—a technology not in general public use at the time—to determine whether Danny Kyllo was cultivating marijuana in his home. The Court declared this surveillance unconstitutional, holding that when “the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a ‘search’ and is presumptively unreasonable without a warrant.”

More recently, the Court revived its emphasis on the Fourth Amendment’s original interpretation to protect against the government’s physical intrusion into a constitutionally protected area in United States v. Jones. There, the Court unanimously held that the warrantless installation of a GPS tracking device on the defendant’s car violated the Fourth Amendment because it constituted a physical invasion of private property.

37. Id. at 361 (Harlan, J., concurring); Carpenter v. United States, 585 U.S. 296, 304 (2018) (applying the reasonable expectation of privacy test).
42. Id. at 29–30.
43. Id. at 40.
44. 565 U.S. 400 (2012).
45. Id. at 406–08. A judge issued a warrant and authorized the government to install the GPS
Writing in concurrence, Justice Sotomayor emphasized her concern that law enforcement’s warrantless use of advanced GPS technology violates an individual’s reasonable expectation of privacy because it “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,” which “chills associational and expressive freedoms” guaranteed to Americans by the Constitution. The analysis presented in Justice Sotomayor’s concurrence later became known as the “mosaic theory,” which seeks to determine “whether a series of acts that are not searches in isolation amount to a search when considered as a [whole].” Justice Sotomayor further suggested that because of the nature of modern surveillance technology, “it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties” under the third-party doctrine.

C. The Third-Party Doctrine’s Extra Layer

The genesis of the third-party doctrine occurred one year before the Court decided Katz in Hoffa v. United States. There, the Supreme Court held that although the Fourth Amendment protects an individual from unwarranted governmental surveillance in their home, office, and even a hotel room, it does not protect an individual’s knowing and voluntary confessions to a third party who may later disclose that information to the police.

One decade later, the Court decided United States v. Miller, formally introducing the third-party doctrine to Fourth Amendment jurisprudence. This doctrine asserts that an individual does not have a reasonable or legitimate

tracking device in the District of Columbia within ten days, but the agents did not execute the warrant until the eleventh day in Maryland. Id. at 402–03. Furthermore, the device monitored the defendant’s location consistently and precisely for twenty-eight days. Id. at 403.

46. Id. at 415–16 (Sotomayor, J., concurring).
47. Orin S. Kerr, The Mosaic Theory of the Fourth Amendment, 111 Mich. L. Rev. 311, 320 (2012); see also Riley v. California, 573 U.S. 373, 394 (2014) (highlighting that “[t]he sum of an individual’s private life can be reconstructed [from their cell phones] through a thousand photographs labeled with dates, locations, and descriptions.”).
50. Id. at 302–03 (emphasizing that the Fourth Amendment does not protect “a wrongdoer’s misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.” (emphasis added)).
expectation of privacy in information they voluntarily share with third parties.\textsuperscript{52} Specifically, in \textit{Miller}, the Court concluded that an individual has no reasonable expectation of privacy in financial statements voluntarily conveyed to their banks.\textsuperscript{53} A few years later, the Court in \textit{Smith v. Maryland} held that an individual does not have a reasonable expectation of privacy in the phone numbers they dial because they voluntarily convey the numerical information to a telephone company and thereby assume the risk that the company could turn over that information to the police.\textsuperscript{54}

In response to the \textit{Smith} majority, Justice Marshall wrote a dissent that hauntingly foreshadowed the consequences of the Court’s third-party doctrine jurisprudence as it existed up until that point.\textsuperscript{55} Justice Marshall asserted that there are some “contexts where, as a practical matter, individuals have no realistic alternative” than to use telephone technology.\textsuperscript{56} Justice Marshall argued that the imperative use of certain technologies to function efficiently in modern society makes the use of such technology a practical necessity rather than a voluntary action.\textsuperscript{57}

Today, Justice Marshall’s dissent holds particular salience: we live in a digital age where 97% of Americans own a cell phone, making it arguably impossible to function in today’s society without one.\textsuperscript{58} According to a 2023 study of cell phone usage statistics, Americans spend on average four hours per day on their phones, and more than half of Americans have never spent more than twenty-four hours without their phones.\textsuperscript{59} In many ways, cell phones have become almost like an individual’s own appendage: 89% of Americans “check their phones within the first [ten] minutes of waking up,” 75% “check their phones within five minutes of receiving a notification,” and 47% of Americans say they feel “panic or anxiety” when their phone battery

\begin{itemize}
  \item \textsuperscript{52} \textit{Id.}
  \item \textsuperscript{53} \textit{Id.} at 442.
  \item \textsuperscript{54} 442 U.S. 735, 744 (1979). Here, law enforcement installed a pen register at the telephone company’s offices to record the numbers the defendant called from his home. \textit{Id.} at 737. The Court concluded that law enforcement’s actions were lawful because the pen register collected only phone numbers rather than the contents of the communication. \textit{Id.} at 741–42.
  \item \textsuperscript{55} \textit{Id.} at 748–52 (Marshall, J., dissenting).
  \item \textsuperscript{56} \textit{Id.} at 750 (Marshall, J., dissenting).
  \item \textsuperscript{57} \textit{Id.} (Marshall, J., dissenting).
  \item \textsuperscript{58} \textit{Mobile Fact Sheet}, PEW RES. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/mobile/ (finding 85% of Americans own a smartphone in particular).
  \item \textsuperscript{59} Alex Kerai, 2023 \textit{Cell Phone Usage Statistics: Mornings Are for Notifications}, REVIEWS.ORG (July 21, 2023), https://www.reviews.org/mobile/cell-phone-addiction/ (using a sample of 1,000 American adults weighted to reflect the characteristics of the American population).
\end{itemize}
Undoubtedly, the pervasive and intimate nature of modern cell phone technology, as Justice Sotomayor alluded to in her Jones concurrence, far exceeds that of the wired telephone used by in 1979 when the Court decided Smith. Indeed, the unanimous Court in Riley v. California held that the government must obtain a warrant before searching the contents of a suspect’s cell phone because:

Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee’s person . . . [M]any of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.

In Riley, the Court underscored the wealth, breadth, and depth of information contained in modern cell phones, distinguishing cell phones from other objects an arrestee might have on their person such as a wallet or car keys.

III. CURRENT STATE OF THE LAW: THE CARPENTER FRAMEWORK AND AMERICAN PRIVACY STATUTES

A. The Technological Exceptionalism Recognized by Carpenter

Although the Court progressively molded its Fourth Amendment jurisprudence to adapt to ever-changing government surveillance technology, it did not adequately address the quickly progressing cell phone technology until 2018 when it decided Carpenter v. United States. There, in an investigation for armed robbery, the FBI—without a warrant—compelled the defendant’s

60. Id.


63. Id.

64. See supra Section II.B.

65. 585 U.S. 296, 309–10 (2018) (holding that an individual has a reasonable expectation of privacy in their physical movements captured by a third party’s storage of cell-site location information).
wireless carrier to disclose transactional records that revealed the date and
time of the defendant’s calls and his approximate location based on cell-site
location information.\textsuperscript{66} In the face of this unprecedented warrantless procure-
ment of advanced and personal technological information, the Court deter-
mined that “individuals have a reasonable expectation of privacy in the whole
of their physical movements,”\textsuperscript{67} especially considering how precise modern
location technology has become.\textsuperscript{68}

Thus, the Court in \textit{Carpenter} narrowed the third-party doctrine’s scope
and concluded that “information about the location of cell phone customers
held by cell phone providers is now protected by the Fourth Amendment [from
government actors], at least when the police seek seven days or more of such
information.”\textsuperscript{69} Thus, \textit{Carpenter} recognized the unprecedented nature of
modern technology like smartphones and the internet as compared to previous
technological advancements with which the Court grappled—it recognized
the modern digital era’s technological exceptionalism.\textsuperscript{70}

\textbf{B. The Carpenter Framework}

Although the Court limited its holding to cell-site location information, it
provided a framework that seeks to answer: “First, does the individual whose
information has been obtained have a reasonable expectation of privacy in the
database? Second, even if that information has been collected and is being
maintained by a private third party, does the third-party doctrine apply?”\textsuperscript{71}
Under the \textit{Carpenter} framework, courts may consider several factors—though
scholars differ on the exact number.\textsuperscript{72} Constitutional law scholar Paul Ohm
highlights three characteristics of cell-site location information noted by the
\textit{Carpenter} majority that could be applied to other data: “(1) ‘the deeply re-
vealing nature’ of the information; (2) ‘its depth, breadth, and comprehensive
reach’; and (3) ‘the inescapable and automatic nature of its collection’” as

\textsuperscript{66} Id. at 300–03.
\textsuperscript{67} Id. at 310.
\textsuperscript{68} Id. at 311–12 (“[W]hen the Government tracks the location of a cell phone it achieves near
perfect surveillance, as if it had attached an ankle monitor to the phone’s user.”).
\textsuperscript{69} Ohm, supra note 11, at 358.
\textsuperscript{70} Id. at 399 (“The beating heart of the \textit{Carpenter} majority opinion is its deep and abiding belief
in the exceptional nature of the modern technological era.”).
\textsuperscript{71} Id. at 369–70.
\textsuperscript{72} For example, Paul Ohm provides three factors and Laura Hecht-Felella provides five. \textit{See id.}
at 369–78; \textit{Hecht-Felella, supra} note 29, at 9–11.
applied to the category of information being sought.\textsuperscript{73}

The first suggested factor protects the “deeply revealing” intrinsic nature of the information about a person, such as their “familial, political, professional, religious, and sexual associations” and other “privacies of life.”\textsuperscript{74} In other words, this factor analyzes whether the government gathered sensitive and intimate information.\textsuperscript{75} It weighs in favor of a finding of a person’s reasonable expectation of privacy in information conveyed to a third party if that information has a “particularly intimate or sensitive and revealing” nature.\textsuperscript{76}

The second factor also analyzes the intrinsic nature of the information but instead focuses on its depth, breadth, and comprehensiveness.\textsuperscript{77} Depth refers to the detail and precision of the information stored, which reveals accurate information about a person’s activities.\textsuperscript{78} Breadth measures “how frequently the data is collected” over time.\textsuperscript{79} Finally, comprehensiveness analyzes the “number of people tracked in the [third-party] database.”\textsuperscript{80}

The third factor examines the “inescapable and automatic nature” of how the information is collected, which looks at “whether the targets of the surveillance may have assumed the risk of the data collection or knowingly exposed their information to the private party.”\textsuperscript{81} The “inescapable” notion attempts to remedy Justice Marshall’s concern in \textit{Smith v. Maryland} that the third-party doctrine mistakenly assumes the voluntariness of technology use when, in reality, using certain technology—e.g., a cellphone or computer—is necessary to function in modern society.\textsuperscript{82} In contrast, the “automatic nature” notion refers to the idea that many forms of data collection do not provide an “opt out” option for users.\textsuperscript{83} This is a gray area for mobile apps, which are voluntarily downloaded.\textsuperscript{84}

\textsuperscript{73} Ohm, supra note 11, at 370 (quoting \textit{Carpenter}, 585 U.S. at 320).
\textsuperscript{75} Ohm, supra note 11, at 371–72.
\textsuperscript{76} \textit{Hecht-Felella}, supra note 29, at 10.
\textsuperscript{77} Ohm, supra note 11, at 372–73.
\textsuperscript{78} \textit{Id.} at 372.
\textsuperscript{79} \textit{Id.}
\textsuperscript{80} \textit{Id.} at 373.
\textsuperscript{81} \textit{Id.} at 376.
\textsuperscript{82} \textit{Smith v. Maryland}, 442 U.S. 735, 749 (1979).
\textsuperscript{83} Ohm, supra note 11, at 377.
\textsuperscript{84} \textit{Id.} at 378 (“[L]ower courts might have difficulty applying this factor to technologies that collect data automatically, but not inescapably—such as mobile apps that are voluntarily downloaded and
In addition to Ohm’s three factors, Brennan Center Liberty and National Security Fellow Laura Hecht-Feella suggests two additional factors in her framework: expense and retrospectivity. Expense refers to the government’s ability to conduct precise in-depth investigations for a cheaper price than would have otherwise been possible through more-traditional surveillance techniques. Additionally, retrospectivity applies “when a technology or data set creates an infallible record that allows the government to effectively travel back in time.” Ohm and Hecht-Feella’s factors fit together nicely and provide a clear roadmap for the Fourth Amendment analysis below in Section IV.B.

C. Praise and Criticism for Carpenter

Because of Carpenter’s deviance from the traditional third-party doctrine, scholars’ reactions to it were both positive and negative. On the one hand, proponents of the new Carpenter test praise it as a milestone in privacy law in the current technological age. Such proponents celebrate Carpenter for its shift in focus from the character of the investigatory techniques to the “nature of the information” obtained by the government that can reveal deeply personal intimacies in which someone would have a reasonable expectation
of privacy.91

On the other hand, critics argue that although Carpenter represents excellent strides in the direction of protecting privacy in the modern world, the narrow ruling only applies to cell-site location information and “would not require law enforcement, in most cases, to obtain a warrant when seeking information held by third-party companies.”92 With that criticism in mind, it is important to address whether current federal and/or state American privacy statutes adequately address the gap between cell-site location information—which is protected under Carpenter—and other private information obtained by third parties—which is not expressly covered by Carpenter.93

D. Current Federal and State Privacy Statutes

Until the European Union’s General Data Protection Regulation (GDPR) took effect in 2018, governments around the world had not yet implemented comprehensive data privacy legislation to protect individuals from the ever-increasing collection of private information by companies.94 The GDPR “imposes[ed] limits on the collection and processing of personal data,”95 pioneering international privacy law.96 More specifically, the GDPR “requires companies to ask for some permissions to share data and gives individuals rights to access, delete, or control the use of that data.”97

In contrast, the United States does not have a comparable comprehensive national privacy law,98 but instead takes a “sectoral” approach to data privacy

---

91. Ohm, supra note 11, at 364; see also United States v. Jones, 565 U.S. 400, 415–16 (2012) (Sotomayor, J., concurring) (articulating that the precision of modern technological data could reveal deeply personal and private intimacies of an individual’s life).
92. Cristina Del Rosso & Carol M. Bast, Protecting Online Privacy in the Digital Age: Carpenter v. United States and the Fourth Amendment’s Third-Party Doctrine, 28 CATH. U. J. L. & TECH. 89, 93 (2020); see also Daniel De Zayas, Carpenter v. United States and the Emerging Expectation of Privacy in Data Comprehensiveness Applied to Browsing History, 68 AM. U. L. REV. 2209, 2213–14 (2019) (praising the monumental decision, but asserting that Carpenter’s “broad reasoning left several questions unanswered—including the decision’s true scope”).
93. See infra Section III.D.
96. Chander et al., supra note 94, at 1735.
97. Klosowski, supra note 21.
regulations.\textsuperscript{99} This approach likely stems from the nation’s historic prioritization of individual autonomy over big government.\textsuperscript{100} Law professors Danielle Keats Citron and Daniel J. Solove describe privacy law in the United States as “a sprawling patchwork of various types of law, from contract and tort to statutes and other bodies of law.”\textsuperscript{101} The United States government, unlike its European counterpart, has enacted various laws that cover either smaller quantities of personal data or vulnerable populations.\textsuperscript{102} For example, the Health Insurance Portability and Accountability Act (HIPAA) covers only communications between patients and health care providers; the Fair Credit Reporting Act (FCRA) protects information in an individual’s credit report; the Family Educational Rights and Privacy Act (FERPA) enumerates who can access or request students’ education records; and the Electronic Communications Privacy Act (ECPA) prevents unlawful government wiretapping.\textsuperscript{103} Additionally, the federal government considers children a vulnerable population, protected through legislation like the Children’s Online Privacy Protection Rule (COPPA), which limits a company’s ability to collect data from children under the age of thirteen.\textsuperscript{104} This patchwork of privacy laws has engendered criticism in that the current United States model only protects specific types of data in limited, often-outdated circumstances.\textsuperscript{105}

In addition, the United States government primarily relies on the Federal Trade Commission (FTC) to regulate online privacy by bringing enforcement actions against apps and websites that violate their own privacy policies.\textsuperscript{106} The FTC Act requires the FTC to prevent companies from engaging in unfair or deceptive business practices.\textsuperscript{107} Unfortunately, as one critic asserts, the


\textsuperscript{100} Chander et al., \textit{supra} note 94, at 1762.


\textsuperscript{102} Klosowski, \textit{supra} note 21.

\textsuperscript{103} \textit{Id}.

\textsuperscript{104} \textit{Id}.

\textsuperscript{105} \textit{Id}.

\textsuperscript{106} U.S. GOV’T ACCOUNTABILITY OFF., \textit{supra} note 98, at 9.

\textsuperscript{107} 15 U.S.C. § 45(a)(2) (2018) (“The [FTC] is hereby empowered and directed to prevent persons,
FTC enforces only a “regime of informed consent, where it primarily ensures that companies disclose to consumers how the company collects and processes data so that consumers can make an informed decision on whether to accept these terms,” rather than actually regulating how those companies use the data.\textsuperscript{108} Furthermore, as of January 2019, the FTC had not implemented its authority to promulgate regulations relating to internet privacy.\textsuperscript{109} Moreover, even though the FTC possesses relatively broad authority to bring enforcement actions, between July 1, 2008, and June 30, 2018, it brought only 101 internet privacy enforcement actions, most of which it resolved through settlement agreements with the companies without civil penalties.\textsuperscript{110} Critics of the FTC enforcement scheme advocate for an “overarching Internet privacy statute” and believe that the FTC should both promulgate regulations to enhance internet privacy and possess the authority to impose civil penalties on violators.\textsuperscript{111}

In terms of state protections, as of July 2023, only eleven states had enacted comprehensive consumer privacy laws: California, Colorado, Connecticut, Florida, Indiana, Iowa, Montana, Tennessee, Texas, Utah, and Virginia.\textsuperscript{112} California arguably has the strongest privacy legislation, offering private causes of action for California consumers to sue companies that abuse their consumers’ data.\textsuperscript{113} In 2018, the California Legislature passed the California Consumer Privacy Act (CCPA); its amendment, the California Privacy Rights Act (CPRA), took effect in early 2023.\textsuperscript{114} Each one a profoundly

---

\textsuperscript{108} Lancieri, supra note 95, at 21.
\textsuperscript{109} U.S. GOV’T ACCOUNTABILITY OFF., supra note 98, at 11.
\textsuperscript{110} Id. at 21–24. Most of these cases dealt with “first-time violations of the FTC Act,” which settled without civil penalties because the FTC lacks authority to impose civil penalties for a first-time violation. Id. at 21. For example, the FTC investigated the period-tracking app company, Flo, in 2021 for allegedly “sharing personal data collected via the app with companies such as Google and Facebook for marketing and advertising purposes.” Mendolla, supra note 7, at 938. Flo and the FTC settled, and the FTC ordered Flo to “obtain consent from its users before sharing personal data with third parties.” Id.
\textsuperscript{111} U.S. GOV’T ACCOUNTABILITY OFF., supra note 98, at introduction.
\textsuperscript{113} Lancieri, supra note 95, at 22.
impactful piece of privacy law, the CCPA and CPRA constitute the nation’s first comprehensive consumer privacy legislation.\footnote{Id.} The CCPA and CPRA prohibit the sale and sharing of personal information to third parties for advertising and created several consumer rights, including the right to private action,\footnote{Id. § 1798.120.} the right to opt out of the sale of personal information to third parties,\footnote{Id. § 1798.110.} the right to know the personal information collected by a business about the consumer,\footnote{Id. § 1798.121.} and the right to limit use and disclosure of sensitive personal information.\footnote{Id. § 1798.140(ae)(2)(C).} Consumer personal information includes “information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.”\footnote{Id. § 1798.140(v)(1).} Consumer sensitive personal information means data that reveals the identification of a consumer’s social security number, financial information, geolocation, genetic data, and email, mail, or text message information.\footnote{Id. § 1798.140(ae).} The statute even protects “[p]ersonal information collected and analyzed concerning a consumer’s sex life” when a company processes biometric information for the purpose of uniquely identifying a consumer.\footnote{Id. § 1798.150(a)(1).}

Unfortunately, even the CCPA and CPRA have their limitations.\footnote{Id.; see also Tara L. Trifon & Lindsey E. Kress, The Murky Waters of the CCPA’s Private Right of Action: Real and Perceived Ambiguitics Complicating Litigation, LOCKE LORD (Nov. 2020), https://www.lockelord.com/newsandevents/publications/2020/11/the-murky-waters.} For example, the private right of action is only applicable in extremely limited circumstances.\footnote{California Consumer Privacy Act (CCPA), CAL. DEP’T JUSTICE, https://oag.ca.gov/privacy/ccpa (last updated May 10, 2023) (answering “what can I do if I think a business violated the CCPA”).} California’s Department of Justice website blatantly says: “You cannot sue businesses for most CCPA violations.”\footnote{Id.} More specifically, a consumer may only sue a company if the consumer can prove that their “nonencrypted and nonredacted personal information . . . [was] subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business’s violation of the duty to implement and maintain reasonable security
procedures and practices . . . to protect the personal information.”126 In other words, a consumer may recover damages only if (1) the company accessed and disclosed nonencrypted, nonredacted, and personal information, (2) a data breach occurred, and (3) the company failed to implement reasonable security procedures.127 The breadth of these provisions will depend on the extent to which courts interpret them narrowly or broadly as litigation ensues in California.128

Although several privacy experts praise the EU and California for their enactments of data privacy laws, several critics assert that these laws still inadequately enforce the bold ambitions of legislators, as companies violate the provisions with little to no consequences.129 Additionally, state privacy laws apply only to those states’ residents, which means that those laws do not protect every American citizen, and conflicting laws might create confusion for companies when they try to comply with privacy statutes.130 Furthermore, the CCPA and CPRA apply exclusively to the sale or exchange of personal information between private parties, rather than information exchanged with or between government actors, making personal and intimate data obtained by private companies still susceptible to government subpoena in criminal investigations.131

If Congress drafts comprehensive federal data privacy legislation in the future, it should follow California’s lead in defining and protecting sensitive personal information, but it should also write a provision that requires law enforcement to secure a warrant before obtaining that sensitive personal information from third-party businesses. A new federal law would also need to address some of California’s shortcomings by expanding the types of private actions that individuals can bring against companies that distribute their personal information.132 A comprehensive federal framework based on this

127. Id.; see also Trifon & Kress, supra note 124.
128. Trifon & Kress, supra note 124.
129. See Klosowski, supra note 21; see also CAL. CIV. CODE § 1798.145(a)(1)(B) (West 2023) (“The obligations imposed on businesses by this title shall not restrict a business’s ability to . . . [c]omply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.”).
130. Klosowski, supra note 21.
131. California Consumer Privacy Act (CCPA), OFF. ATT’Y GEN., https://oag.ca.gov/privacy/ccpa (last visited Jan. 14, 2024); see also CAL. CIV. CODE § 1798.145(a) (West 2023) (stating that the CCPA and CPRA will not restrict business’ obligation to comply with the law, court orders, or subpoenas).
132. See Trifon & Kress, supra note 124 (noting the shortcomings of CCPA); Mendolla, supra note
model, coupled with effective enforcement policies, would provide more consistent and predictable protections and requirements for consumers and companies across the nation, and it would address the criticism that the United States’ current sectoral, patchwork approach provides confusing and outdated policies and protections.133

IV. PRIVACY AND PERIOD-TRACKING APPS IN A POST-DOBBS NATION

Nothing reflects the current digital smartphone age better than the slogan “there’s an app for that.”134 Chief Justice Roberts, writing for a unanimous Court in *Riley*, best summarized the potency of apps:

[Apps] offer a range of tools for managing detailed information about all aspects of a person’s life. There are apps for Democratic Party news and Republican Party news; apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; apps for tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; apps for improving your romantic life.135

The apps we download onto our smartphones paint incredibly intimate portraits of our daily lives, including our political beliefs, financial information, and health data.136 Each app, taken together, precisely reconstructs an individual’s “familial, political, professional, religious, and sexual associations” in one device.137 As this Part argues, the massive, intimate nature of modern technology—coupled with the new possibility of criminal abortion

---

133. See generally Klosowski, supra note 21 (arguing that the current federal privacy framework “target[s] only specific types of data in special (often outdated) circumstances,” unlike the European GDPR, which requires companies “to ask for some permissions to share data and gives individuals rights to access, delete, or control the use of that data”); Safreed, supra note 99, at 123 (discussing the current “patchwork” of federal privacy laws).


136. *Id.*

prosecutions following *Dobbs*—has critical implications for the application of the Fourth Amendment and privacy statutes to period-tracking apps.\textsuperscript{138} Compare the intimate and advanced nature of technology today with that used by pre-*Roe* women who sought abortions.\textsuperscript{139} Before Illinois legalized abortion after *Roe v. Wade*, the Jane Collective provided illegal abortions to women unable to travel to another state (largely because they could not afford to) which, in turn, made abortions only available to women who came from wealthy backgrounds.\textsuperscript{140} This left poor women—largely women of color—with no choice but to conduct dangerous self-induced abortions or to seek illegal “back-alley” abortionists, resulting in an estimated 5,000 deaths from botched abortions per year.\textsuperscript{141}

The Janes advertised their services by printing in alternative and student newspapers with the slogan: “Pregnant? Don’t want to be? Call Jane.”\textsuperscript{142} Women desperate for an abortion called the number attached to the advertisement and left a voicemail.\textsuperscript{143} A “Callback Jane” would reach out to the caller to collect her information on an index card with her name and address, which was then passed along to a “Big Jane” who decided whether to provide the abortion.\textsuperscript{144} If they decided to accept the patient, the Janes first took the patient to a location called “The Front” for a consultation, then blindfolded the patient before taking her to another location called “The Place,” where they performed the abortion.\textsuperscript{145} Eventually, in 1972, the Chicago Police Department caught the Janes’ operation and arrested seven of them for violating Illinois’s anti-abortion laws.\textsuperscript{146} After *Roe v. Wade* recognized a right to abortion one year later, the state of Illinois dropped its charges against the Janes, and the organization—now no longer needed—faded into oblivion.\textsuperscript{147}

Although the Janes went under the radar for several years in the 1960s and 1970s, a similar operation would likely get caught and disbanded

\textsuperscript{138} See infra Sections IV, B–C.
\textsuperscript{139} Haberman, supra note 1.
\textsuperscript{140} Recker, supra note 13.
\textsuperscript{142} See Haberman, supra note 1.
\textsuperscript{143} Id.
\textsuperscript{144} Id.
\textsuperscript{145} Id.
\textsuperscript{146} Id.
\textsuperscript{147} Id.
immediately today. After all, “location history is available both through digital device extractions and subpoenas,” which law enforcement could use to determine the possible location of an underground abortion clinic. Furthermore, law enforcement can use geofencing, “an advertising tool used to market products based on the consumer’s location,” to target clinics based on the location of people suspected of obtaining abortions. Additionally, the government could use social media activity, internet search history, and wearable devices—e.g., Apple Watches or Fitbits—to gather evidence of the whereabouts of women seeking abortions and the possible locations of clinics. Finally, law enforcement and prosecutors could theoretically obtain menstrual information from period-tracking app companies to determine whether a woman suddenly menstruated again after a few months without a period.

Fifty years ago, the most comparable piece of technology to that of today was the telephone that women used to call the Janes’ number. Back then, the Supreme Court had not yet decided Smith, which concluded that the government can subpoena third-party telephone companies only for the numbers dialed; thus, no binding constitutional authority existed that would have expressly permitted the government to subpoena dialed phone numbers from telephone companies. But things are different today than they were fifty years ago.

Because of the sensitive nature of modern information collected from smartphones, many apps encrypt their users’ data as a privacy measure to protect digital data confidentiality. Those encryption measures raise new questions about the privacy protections available for sensitive, intimate app data.

148. See, e.g., Conti-Cook, supra note 8, at 51–56 (identifying different types of digital resources law enforcement can use to build a case against pregnant people).
149. Id. at 51.
150. Id. Interestingly, “[g]eofencing tools have already targeted people entering and leaving Planned Parenthood clinics across the country, sending them anti-abortion messages via their search browser on their digital devices.” Id.
151. Id. at 54–55, 73. Digital history has become increasingly compromised through the spreading of medical information among health providers, device applications, insurance companies, and employers. See id. at 73.
152. Id. at 48.
153. See Haberman, supra note 1.
156. See infra Sections IV.A–C.
A. Encryption and Period-Tracking Apps

Turning to one nuance of the modern technological age, this section introduces a possible application of Fourth Amendment jurisprudence to data encryption.157 With sensitive personal information on smartphones and computers, encryption provides an important way to protect that information using a mathematical technique called “cryptography.”158 This technique converts the original plaintext into “ciphertext,” making it unreadable without the proper “key” to decipher it.159 Using a binary key or password, an authorized user can decrypt the data and read it.160

In response to Dobbs and the abortion trigger laws in more conservative states, several period-tracking apps assured their users of their data’s privacy and encryption protection.161 These assurances may be misleading because companies could still share users’ personal data to other companies.162 And although the Fourth Amendment likely cannot prevent the government from decrypting ciphertext that it lawfully possesses,163 the privacy interests described in Carpenter’s central holding may provide a useful analysis, particularly as applied to whether users of period-tracking apps have a reasonable expectation of privacy in the personal data entered into their encrypted apps.164

157. See infra Sections IV.A–C.
159. Id.
160. Id.
161. See Ropek, supra note 5 (introducing the new protocols of period-tracking app Stardust to protect user information from government tracking); Alisha Haridasani Gupta & Natasha Singer, Your App Knows You Got Your Period. Guess Who It Told?, N.Y. TIMES (Jan. 28, 2021), https://www.ny-times.com/2021/01/28/us/period-apps-health-technology-women-privacy.html (discussing that several apps, including the period-tracking app Flo, have failed to keep their promises to users by mishandling private data).
162. Ropek, supra note 5 (explaining that assurances made by period-tracking companies may not guarantee the protection of users’ data for third party purposes).
163. Orin S. Kerr, The Fourth Amendment in Cyberspace: Can Encryption Create a “Reasonable Expectation of Privacy?,” 33 CONN. L. REV. 503, 517 (2001). Professor Kerr argues that the act of decrypting ciphertext does not itself violate Fourth Amendment privacy expectations because the Fourth Amendment regulates government access to encrypted data, not government efforts to translate ciphertext into plaintext. Id. at 505.
164. See infra Sections IV.B–C.
B. The Third-Party Doctrine and Encrypted Period-Tracking Apps

To reiterate, the Supreme Court concluded in *Miller* and *Smith* that an individual has a diminished expectation of privacy in information voluntarily disclosed to a third party.\(^{165}\) But because *Carpenter* concluded that an individual possesses a reasonable expectation of privacy in cell-site location information, in light of the intimate and precise nature of modern data collection, this Comment argues that *Carpenter*’s holding should embrace new applications, particularly in the context of apps.\(^{166}\) In order to apply *Carpenter* to period-tracking apps, this Comment will apply the factors established by Ohm and Hecht-Felella introduced in Section III.B: “(1) ‘the deeply revealing nature’ of the information; (2) ‘its depth, breadth, and comprehensive reach’; [] (3) ‘the inescapable and automatic nature of its collection’” as applied to the category of information being sought; (4) expense; and (5) retrospectivity.\(^{167}\)

Courts may consider the first factor: the “deeply revealing” nature of the information about a person, such as their sexual associations.\(^{168}\) American women and adolescents use period-tracking apps that collect private reproductive information concerning their menstrual cycles, fertility, pregnancy, and menopause.\(^{169}\) A poll demonstrated that 58% of women have felt embarrassment while menstruating, 42% have experienced period shaming, and 12% have felt shamed by a family member.\(^{170}\) This personal, and oftentimes embarrassing, data is precisely the type of “deeply revealing” information about an individual’s reproductive health and sexual associations, arguably


\(^{167}\) See Ohm, *supra* note 11, at 370 (providing the first three factors); HECHT-FELELLA, *supra* note 29, at 9–10 (providing the expense and retrospectivity factors); *supra* Section III.B.


\(^{169}\) Danielle Keats Citron, *A New Compact for Sexual Privacy*, 62 WM. & MARY L. REV. 1763, 1774–75 (2021); see also Caitlin Riffer, *Note, As Young as Eight: A Post-Dobbs Statutory and Public Policy Solution to Protect Minors’ Reproductive Health Data Online*, 63 WASHBURN L.J. 255, 264–65 (2024) (discussing the protection of minors’ intimate data and stating that “period-tracking applications are the second most popular health app on adolescents’ smartphones.”).

\(^{170}\) Valerie Siebert, *Nearly Half of Women Have Experienced ‘Period Shaming,’* N.Y. POST (Jan. 3, 2018), https://nypost.com/2018/01/03/nearly-half-of-women-have-experienced-period-shaming/ (listing results from a study conducted by THINX, a period-proof underwear company, which used a sample of 1,500 women and 500 men from across the United States).
more intimate than their cell-site location information.\textsuperscript{171}

Next, courts can analyze the depth (detail and precision of the information), breadth (frequency of the data collection over time), and comprehensive reach (number of people tracked in the third-party database) of information.\textsuperscript{172} In terms of depth, women who use period-tracking apps “enter, among other things, their weight, temperatures, moods, reading material, sexual encounters, tampon use, alcohol consumption, cigarette and coffee habits, bodily secretions, and birth control pills.”\textsuperscript{173} Some apps even provide other services like “period predictions and health reports that can be shared with doctors.”\textsuperscript{174} Users of period-tracking apps monitor their cycles for several reasons, including bodily awareness, pregnancy planning, understanding their cycles, cycle preparation, and providing information to their doctors.\textsuperscript{175} Additionally, these apps’ data may “explicitly or implicitly include information about dates of abortions and miscarriages.”\textsuperscript{176} As for breadth, period-tracking apps such as Flo encourage women to enter intimate data each day to provide accurate menstrual, health, fertility, pregnancy, and menopause information.\textsuperscript{177} Additionally, the comprehensive reach of individuals who use period-tracking apps in America is quite extensive: nearly one-third of American women use these apps,\textsuperscript{178} and period-tracking apps constituted the “second most popular category of health apps among adolescent” girls in 2016.\textsuperscript{179}

Courts may then analyze the third factor, the “inescapable and automatic nature” of how the information was collected, by looking at “whether the targets of the surveillance may have assumed the risk of the data collection or

\textsuperscript{171} Cf. Jones, 565 U.S. at 415–16 (Sotomayor, J., concurring) (discussing the privacies of life, including one’s “sexual associations”).
\textsuperscript{172} Ohm, supra note 11, at 372–73.
\textsuperscript{173} Citron, supra note 169, at 1775.
\textsuperscript{174} Id. at 1776.
\textsuperscript{176} Fowler & Ulrich, supra note 38, at 1267. Explicitly, these apps might directly collect information from users about miscarriages. \textit{Id.} Implicitly, “[i]f a user has a missed period and then several weeks later resumes menstruating, this data could imply an abortion or a miscarriage.” \textit{Id.} at 1267 n.205.
\textsuperscript{177} See Gupta & Singer, supra note 161; Flo, https://flo.health/about-flo (last visited Jan. 14, 2023) (stating that Flo can assist women in “making sense of [their] periods, getting pregnant . . ., or tracking [their] baby’s growth and development.”).
\textsuperscript{178} Garamvolgyi, supra note 10 (citing to 2019 survey by Kaiser Family Foundation).
\textsuperscript{179} Scatterday, supra note 175, at 640–41; see also Riffer, supra note 169, at 264–65.
knowingly exposed their information to the third party.

One may argue that the collection of data from period-tracking apps differs entirely from the passive collection of cell-site location information by cell phone carriers raised in Carpenter because users voluntarily download the apps and input personal information, thereby impliedly consenting to the apps’ collection and distribution of their data. In particular, some scholars argue that the Fourth Amendment does not provide app users any protection from government surveillance because their “distinguishing characteristic remains the voluntary provision of data [to the app], which eliminates the expectation of privacy.”

Although these arguments raise a valid point about users’ reasonable expectations of privacy, users of period-tracking apps often believe that their data remains anonymous, suggesting that those users do not knowingly expose their private fertility and sexual information, especially if they use an anonymous setting where a user does not provide any personally identifying information—e.g., an email, name, or profile photo. Interestingly, although courts may “rely on consumers’ supposed knowledge of . . . privacy policies addressing the collection or sharing of personal data,” realistically, “users are very unlikely to read their privacy policies,” which refutes the “knowing exposure” critique.

Furthermore, despite a user’s voluntary decision to download a period-tracking app, the use of period-tracking apps nonetheless fulfills the Katz test: a user actually expects that the personal and intimate information will remain in the app (not in the hands of third parties), and such an expectation is one society would be prepared to accept as reasonable because, as in Riley, apps “offer a range of tools for managing detailed information about all aspects of

180. Ohm, supra note 11, at 376.
182. Fowler & Ulrich, supra note 38, at 1290.
184. Tokson, supra note 183, at 174, 149.
a person’s life.”186 Thus, voluntarily inputting fertility information into an app on one’s personal phone does not forfeit a reasonable expectation of privacy to the same extent as disclosing criminal actions to a third party187 or submitting financial statements to a bank.188

Next, regarding one of the two additional factors proposed by Hecht-Felella, the expense factor refers to the government’s ability to conduct precise, in-depth investigations for a cheaper price than more traditional surveillance techniques.189 Recently, the government, in issuing subpoenas to third parties, has become “increasingly aggressive in attempting to force tech companies to turn over users’ private information through forced decryption.”190 As an investigative strategy, such “subpoenas are probably more important than physical searches of homes, businesses, and effects,” because the government can obtain relevant intimate information from a third-party period-tracking app on a lesser burden of proof, rather than expending its resources to obtain a warrant based on probable cause to search the suspect’s phone itself.191

The final factor, retrospectivity, analyzes whether the data obtained by the government creates an “infallible record” that could allow the government to essentially “travel back in time.”192 Period-tracking app companies can store both extensive and long-term data, even if a user deletes the app, thus giving the government an accurate and comprehensive record of a user’s reproductive health trends.193 For example, Flo’s privacy policy reserves the right to retain personal data for a period of three years, even after deleting the app or after a period of inactivity.194 However, even the most secure or private apps could retain users’ data for about thirty days after app deletion.195

Overall, in applying the Carpenter factors, the personal and sensitive

189. HECHT-FELELLA, supra note 29, at 10.
192. See HECHT-FELELLA, supra note 29, at 10.
193. See Fowler & Ulrich, supra note 38, at 1268 (describing privacy issues users may face after deletion of these apps); see also Kristen Poli, The Most Popular Period-Tracking Apps, Ranked by Data Privacy, WIRED (July 20, 2022), https://www.wired.com/story/period-tracking-apps-flo-clue-stardust-ranked-data-privacy/#:~:text=Flo%2C%20whose%20security%20practices%20placed,for%20up%20to%2024%20months%20of%209D.
194. Poli, supra note 193; see also FLO, supra note 183.
195. Poli, supra note 193.
nature of the data placed into third-party period-tracking apps, in addition to the heightened protections afforded by encryption, make that data precisely the type of information that should be protected by the Fourth Amendment because it reveals personal intimacies in which someone would have a reasonable expectation of privacy.196

C. Federal and State Privacy Statutory Protections over Period-Tracking Apps

Even if the Supreme Court agrees with this Comment and extends Carpenter to include intimate data collected by apps, revising federal and state privacy statutes would provide an extra layer of security to users of period-tracking apps because, as they currently stand, the statutes do not provide adequate protection against government access to period-tracking app data.197 Although California has relatively comprehensive privacy protections, the CCPA and CPRA would not provide California users of period-tracking apps with a private cause of action against companies who sell their personal information to the government or other third parties.198 In fact, under the current California privacy scheme, period-tracking app users cannot sue app companies unless an app company’s failure to implement and maintain preventative security measures caused a breach of the users’ unencrypted personal information.199 Furthermore, because the United States lacks comprehensive national data-privacy legislation, period-tracking apps remain highly unregulated.200 This raises particular concern over the ability of third parties to obtain personally identifiable and private information from these companies.201 For example, period-tracking app companies “often sell user data to third parties, which in turn sell that information to data aggregators or brokers.”202 They can also resell this data to law enforcement and intelligence agencies.203 Interestingly, a pregnant woman’s data is of particularly high interest to third

196. See supra Sections IV.A–B.
197. See, e.g., infra Section V.B (arguing that Congress should adopt a comprehensive federal statute to protect intimate data collected by period-tracking apps).
198. CAL. DEP’T JUSTICE, supra note 125 (answering “what can I do if I think a business violated the CCPA”).
200. Scatterday, supra note 175, at 642–43.
201. Id. at 643.
202. Id. at 645.
203. Fowler & Ulrich, supra note 38, at 1265.
parties because insurance companies can use the data sold by period-tracking app companies to “make targeting decisions, such as whether to sell [a woman] a life insurance policy, or how much [her] premium should be.”

For example, Ovia Health, a digital platform that assists with women’s health and family planning, received criticism for sharing anonymized data with employers who could purchase the app as part of an employee health benefit package.

The concerns discussed thus far pertain primarily to the sale of personal data between a period-tracking app company and data brokers—so how does the lack of privacy rights fit into the abortion-prosecution framework?

Some period-tracking app privacy policies expressly state that the companies may share users’ personal data in special circumstances; for example, Flo’s privacy policy states that it “may also share . . . personal data . . . [i]n response to subpoenas, court orders, or legal processes.” Essentially, this means that law enforcement may compel a company to provide information related to a criminal investigation through a subpoena and access an individual’s personal data from period-tracking app companies without a warrant requiring probable cause.

Statistics show that a shockingly few number of people actually read privacy policies: a Pew research survey from 2019 found that only 9% of Americans report that they “always” read privacy policies, and only 13% report that they “often” read privacy policies. Smartphone apps have notoriously long privacy agreements, with one author reporting that the privacy policies for the

---


206. Norman & Knight, supra note 204.

207. MacDonald, supra note 7 (quoting a law professor who expressed her concerns that, “from an evidentiary standpoint, [she] can see how the [period-tracking app] information would be valuable” to the government in criminal abortion prosecutions).

208. FLO, supra note 183.


apps on his phone totaled almost one million words.211 Additionally, in 2008, an engineering and public policy professor “estimated that reading and consent- ing to all the privacy policies on websites Americans visit would take 244 hours per year.”212 These numbers make it highly unlikely that someone who downloads a period-tracking app onto her phone carefully reads the privacy policy, thus leaving users unaware of the reality that the government could serve a subpoena on Flo (or other similar app companies) to obtain personal reproductive-health information rather than a warrant.213

Furthermore, “[d]ata brokers trade in other types of information, such as location-tracking data for people who visited Planned Parenthood, which poten- tially could be purchased by law enforcement.”214 In other words, period- tracking app companies would have a hard time resisting a government sub- poena for reproductive- or fertility-related information in a criminal abortion investigation.215 In fact, a similar issue emerged in 2016 when Apple refused to unlock a shooting suspect’s iPhones pursuant to an FBI investigation.216 While this case raised the issue of whether the government can subpoena private information contained in smartphones, a court never adjudicated the question because the FBI eventually broke into the suspect’s phone without Apple’s assistance, so the legality of the government’s subpoena remains dis- putaed.217

Furthermore, the use of data collected by advertising companies already concerned women who sought abortions pre-Dobbs.218 In 2015, an advertising company in Massachusetts concentrated pro-life advertisements toward “abortion-minded women” when they visited health care professionals.219 The advertising firm used geofencing location technology and website searches to target women’s cell phones so that they would receive a constant stream of pro-life ads.220

211. Id.
212. Id. The professor has not updated her calculation since then, but one can only imagine how much that number has increased in the last fifteen years, especially accounting for the privacy policies for smartphone apps. Id.
213. See id.
214. Norman & Knight, supra note 204.
215. Id.
217. Id.
218. See Citron, supra note 169, at 1808.
219. Id.
220. Id.
In sum, current federal and state privacy laws do not provide comprehensive protection of women’s reproductive data as applied to government subpoenas from app companies. Further, although the Carpenter factors provide useful guidance on how future judges might decide cases concerning government surveillance of period-tracking app data, it remains uncertain whether Carpenter would actually protect the app data, given the Court’s intentionally narrow ruling.

V. IMPACT AND SIGNIFICANCE: RECONCILING CARPENTER AND THE PRIVACY OF APP DATA

Considering the uncertain legacy that follows Carpenter and the lack of adequate privacy statutes currently in effect in the United States, this Part next inquires: (1) whether the current Supreme Court will reconcile Carpenter with issues like government surveillance of individuals through app data, and (2) whether Congress should act to solidify privacy rights for all American citizens.

A. What Would the Current Supreme Court Think?

The composition of the Supreme Court has changed quite a bit since it handed down Carpenter in 2018. Three new Justices have joined the Court: Justices Kavanaugh, Barrett, and Jackson. Chief Justice Roberts authored the Carpenter opinion, joined by Justices

---

221. Id. at 1770–71; see supra discussion in Section IV.C.
222. See Carpenter v. United States, 585 U.S. 296, 315–16 (2018) (“We therefore decline to extend Smith and Miller to the collection of CSLI. Given the unique nature of cell phone location information, the fact that the Government obtained the information from a third part does not overcome Carpenter’s claim to Fourth Amendment protection.”); see also Del Rosso & Bast, supra note 92, at 103 (discussing Carpenter’s narrow ruling and the resulting unanswered questions; for instance, its application in other technological and privacy settings).
223. See infra Sections V.A–B.
224. The following discussion offers a limited and speculative analysis into what the Supreme Court with its current composition would think about expanding Carpenter to private personal information stored on apps.
226. See id.
Kagan and Sotomayor. Three of the Carpenter dissenters who currently sit on the Court—Justices Alito, Gorsuch, and Thomas—rested their dissents on the assertion that the majority’s interpretation of the Fourth Amendment, starting with Katz, is inconsistent with the “text and original understanding of the Fourth Amendment.” Since Carpenter, Justices Kavanaugh and Barrett have joined the conservative originalist majority. Although it would be difficult to predict how the Justices would rule on expanding Carpenter’s application beyond cell-site location information, Professor Matthew Tokson notes that Justice Barrett’s decisions as a lower-court judge “generally ruled in favor of Fourth Amendment protection,” and she “spoke favorably” about the Carpenter decision at her confirmation hearing. Additionally, Tokson opines that Justice Kavanaugh “may be open to broader interpretations of the Fourth Amendment when they are supported by precedent and compelling policy or equitable considerations.” Similarly, as the newest member of the Court, Justice Jackson’s Fourth Amendment jurisprudence is unpredictable because her Fourth Amendment-related cases as a lower court judge did not precisely address Carpenter.

Despite the new composition of the Court, Tokson asserts, “It is likely that Carpenter will remain a valid precedent and that its reasoning will be used to expand the scope of the Fourth Amendment to a variety of new

---

227. Carpenter, 585 U.S. at 299.
228. Id. at 391 (Gorsuch, J., dissenting); see id. at 361–62 (Alito, J., dissenting) (arguing that the majority’s decision “violates both the original understanding of the Fourth Amendment and more than a century of Supreme Court precedent”); id. at 343 (Thomas, J., dissenting) (“The Katz test has no basis in the text or history of the Fourth Amendment.”).
230. Tokson, supra note 225, at 1835–36; see also VALERIE C. BRANNON ET AL., CONG. RESEARCH SERV., R46562, JUDGE AMY CONEY BARRETT: HER JURISPRUDENCE AND POTENTIAL IMPACT ON THE SUPREME COURT 38 (2020) (stating that Justice Barrett “frequently joined Fourth Amendment opinions constraining the government’s ability to conduct warrantless searches”).
231. Tokson, supra note 225, at 1836; see also Orin Kerr, Judge Kavanaugh on the Fourth Amendment, SCOTUSBLOG (Jul. 20, 2018), https://www.scotusblog.com/2018/07/judge-kavanaugh-on-the-fourth-amendment/#:~:text=Kavanaugh%20filed%20two%20warrantless%20warrantless%20searches,Maryland (describing then-Judge Kavanaugh’s Fourth Amendment jurisprudence as “modest”).
technologies and surveillance practices.” But, he also acknowledges that “the future is uncertain” and until the Court confronts a case challenging Carpenter, Americans will not know the answer. Given the unpredictability of Carpenter’s legacy, it is imperative that Congress unites to protect Americans with a comprehensive federal privacy statute.

B. A Call to Action for Congress to Codify National Privacy Legislation

Because the legacy of Carpenter remains somewhat unclear, the optimal path forward for data protection is for Congress to pass a comprehensive federal statute that would require the government to obtain a warrant before accessing personal and intimate information held by third-party app companies. Alternatively, as one scholar suggests, Congress should enact comprehensive privacy legislation that limits the collection and use or sale of intimate information without users’ consent. As another possible solution, Congress could update HIPAA “to encompass consumer health technologies like [period-tracking apps] within the definition of a covered entity.”

In 2018 and 2019, there were at least ten federal privacy bills proposed in Congress that never saw the light of day. In 2021, a group of senators introduced a bipartisan bill called the “Fourth Amendment Is Not For Sale Act” (FANFSA) in an effort for Congress to pass legislation that prohibits law enforcement from warrantlessly accessing digital information held by data brokers on smartphone apps. FANFSA “would require the government to obtain court orders before compelling data brokers to disclose personal user data” to prevent law enforcement from “bypassing the Carpenter warrant process by purchasing data from third-party data brokers.”

Unfortunately, this

233. Tokson, supra note 225, at 1833.
234. Id.
235. See infra Section V.B.
238. Fowler & Ulrich, supra note 38, at 1296.
The bill has not yet come to fruition and would only prevent the government from obtaining information from data brokers, not necessarily from the apps or companies who sell the data themselves.  

A comprehensive national policy should protect information like private health-related menstrual data and prohibit the government from accessing that information without either the express consent of the individual or a search warrant supported by probable cause. For example, Congress could add defining language similar to (but improved from) the CCPA and CPRA, such as: “sensitive personal information includes: individual health and reproductive data entered into a third-party app.” Additionally, the federal statute should require law enforcement to obtain a warrant before accessing personal sensitive information to correct the exemption in the CCPA and CPRA that allows third-party companies to disclose sensitive personal information to law enforcement pursuant to a subpoena. Thus, law enforcement would still have the ability to access period-tracking information, but only upon demonstrating probable cause for the information, which would prevent intrusive government rummaging into personal data.

C. Impacts and Consequences for Users of Period-Tracking Apps

In her article, Professor Danielle Keats Citron advances a persuasive argument for why intimate sexual data imperatively needs protection in a modern society and why dangers arise from the current norms for handling and distributing that data. She asserts that “private-sector surveillance of intimate information imperils self-expression and the ability of people to explore new information and ideas,” which may cause people to “not use period-tracking apps that help them manage anxiety, pain, and uncertainty.” Unfortunately, because data brokers can sell users’ information to third parties, this

242. See id. at 93. The House Judiciary Committee passed the bill in July 2023, but has not made progress since. Id.

243. See supra Section IV.C.

244. See, e.g., CAL. CIV. CODE § 1798.140(ae) (West 2023) (defining “sensitive personal information”).

245. See, e.g., id. § 1798.145(a)(2) (listing exemptions).

246. Cf. Wasserstrom & Seidman, supra note 30, 54–55 n.142 (highlighting that the Founding generation intended the Fourth Amendment to require specificity from law enforcement when obtaining information during investigations).

247. See Citron, supra note 169.

248. Id. at 1793–94.
private-sector surveillance not only prevents people from accessing important resources but also poses detrimental impacts on an individual’s reputation, employment, and insurance opportunities.\textsuperscript{249}

As for abortion prosecutions, before the Court decided \textit{Dobbs} in June 2022, Ford Foundation Technology Fellow Cynthia Conti-Cook predicted that several American women would “turn[] to the internet for medical advice” to identify options for reproductive health care.\textsuperscript{250} And considering that national privacy law does not adequately protect personal information, law enforcement has access to these “digital trails” for abortion prosecutions.\textsuperscript{251} For instance, Conti-Cook asserts that:

\begin{quote}
A wide variety of digital forensic technology and other forms of technology broaden state surveillance power through online searches, geofencing, location tracking, purchasing history, and more. Combined, these data points could identify, for example, the profiles of pregnant people spending time at substance abuse treatment centers, making purchases at bars, or repeatedly taking a particular route across state lines.\textsuperscript{252}
\end{quote}

Conti-Cook’s description of how law enforcement might collect evidence in an abortion investigation parallels the “mosaic theory” of Fourth Amendment searches discussed in Section II.B.\textsuperscript{253} To briefly reiterate, the mosaic theory asserts that searches of several individual pieces of information alone might not paint an intimate picture but, taken together, could reveal a wealth of information about a person’s whereabouts.\textsuperscript{254}

Actual law enforcement practices evidence this theory: prosecutors already use digital trails as evidence in trials.\textsuperscript{255} For example, the government obtained a woman’s online searches for abortion pills, in addition to unencrypted text messages to a friend about her unwanted pregnancy and the abortion pills she purchased.\textsuperscript{256} Based on this evidence, the government charged

\begin{itemize}
\item \textsuperscript{249} \textit{id.} at 1799; \textit{see also} Norman \& Knight, \textit{supra} note 204.
\item \textsuperscript{250} Conti-Cook, \textit{supra} note 8, at 5.
\item \textsuperscript{251} \textit{id.} at 6.
\item \textsuperscript{252} \textit{id.} at 6–7.
\item \textsuperscript{253} \textit{See supra} Section II.B.
\item \textsuperscript{254} Kerr, \textit{supra} note 47, at 320.
\item \textsuperscript{255} Conti-Cook, \textit{supra} note 8, at 6, 49–51.
\item \textsuperscript{256} Patel \textit{v.} Indiana, 60 N.E.3d 1041, 1045 (Ind. Ct. App. 2016).
\end{itemize}
her with neglect of a dependent and felony feticide, using evidence of her online research for abortion pills and unencrypted text messages. 257

Therefore, scholars rightly worry that the individual data points collected on someone suspected of obtaining an abortion may come together to form a deeply incriminating case as a whole. 258 Considering how much information people store on cell phones and computers, law enforcement’s ability to access one piece of information can potentially open the floodgates for other types of information because “the sum of an individual’s private life can be reconstructed” from their digital devices. 259

VI. CONCLUSION

Since the 1960s, the Supreme Court has expanded our understanding of the Fourth Amendment to encompass a personal right to privacy in the context of ever-changing law enforcement surveillance and technological developments. 260 The Court’s decision in Carpenter elicited praise for its recognition of modern-day technological exceptionalism, with scholars considering it a milestone in Fourth Amendment jurisprudence. 261 The Court in Carpenter recognized that cell-site location information paints a highly intimate portrait of an individual’s movements for long spans of time, thus requiring constitutional protection. 262 Meanwhile, critics of Carpenter argue that the decision did not go far enough, as it failed to encompass all digital information and

257. Id. at 1044–45.
258. See, e.g., Conti-Cook, supra note 8, at 51.
260. See Katz v. United States, 389 U.S. 347, 351–53 (1967) (expanding Fourth Amendment protection beyond physical trespass to include any invasion upon an individual’s reasonable expectation of privacy); United States v. Miller, 425 U.S. 435, 442 (1976) (applying the Katz test to bank records); Smith v. Maryland, 442 U.S. 735, 744 (1979) (holding that the use of a pen register to collect information from third-party phone company was not a “search” within the meaning of the Fourth Amendment); Kyllo v. United States, 533 U.S. 27, 40 (2001) (holding that the use of thermal-imaging technology to search home violated the Fourth Amendment); United States v. Jones, 565 U.S. 400, 404 (2012) (holding that the Fourth Amendment prohibits the extended tracking of a vehicle through a surreptiously installed GPS-tracking device); Riley, 573 U.S. at 386 (finding that searches of cell phones warrant special Fourth Amendment considerations); Carpenter v. United States, 585 U.S. 296, 309–10 (2018) (finding that the third-party doctrine does not negate Fourth Amendment protection against government acquisition of cell-site location information).
261. Carpenter, 585 U.S. 309–10; Ohm, supra note 11, at 358; see also Laperruque, supra note 90 (“[T]he Carpenter ruling represents a huge leap forward for privacy rights in public.”).
262. See supra Section III.A.
does not cover government subpoenas of third-party app companies.263
Because the Court narrowly limited its ruling in Carpenter to cover only cell-site location information, and because it is unknown whether the new members of the Court will vote to expand Carpenter to other digital information,264 this Comment argues first that in the essence and spirit of Carpenter—in recognition of today’s unprecedented “technological exceptionalism”—the Supreme Court should extend Ohm and Hecht-Felella’s factor-based tests to the intimate personal information placed into smartphone apps.265 In writing the Fourth Amendment, the Founders intended to protect Americans from general warrants and government invasions into their personal belongings and property.266 The text of the Fourth Amendment itself guarantees “[t]he right of the people to be secure in their . . . effects, against unreasonable searches and seizures.”267 Thus, the text of the Amendment support the notion that the term “effects” should cover a cell phone as an “effect” that warrants constitutional protection.268
Furthermore, regardless of whether the Supreme Court does extend Carpenter to other types of digital evidence, this Comment urges Congress to pass a more comprehensive federal statute.269 As discussed in Section III.D, the current landscape of American privacy legislation largely falls in the hands of the states, which in turn results in inconsistent and oftentimes confusing applications for Americans across the nation, leaving app companies largely unregulated.270 A comprehensive federal statute, as suggested in Section V.B, should protect intimate personal app data by defining sensitive personal information and barring the government from obtaining the information without a warrant or consent.271

263. Del Rosso & Bast, supra note 92, at 107; De Zayas, supra note 92, at 2214, 2254.
264. See Tokson, supra note 225, at 1833–36 (discussing the future of Carpenter at the Supreme Court now that the Court’s composition has changed since its decision in 2018).
265. See supra Section IV.B.
266. Wasserstrom & Seidman, supra note 30, at 54–55 n.142.
268. See Riley v. California, 573 U.S. 373, 403 (2014) (“Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans ‘the privacies of life.’[.] The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought.”).
269. See supra Section V.B.
270. See supra Section III.D.
271. See supra Section V.B.
Ultimately, regardless of one’s moral, political, and constitutional opinions about abortion, we live in a reality where the government can access extremely private digital reproductive data without a warrant, subjecting women who live in abortion-restrictive states to intrusive government surveillance that violates their reasonable expectations of privacy.272

Until the Supreme Court or Congress guarantees federal protection against this kind of intrusive government searching, we must live with the reality that private personal data we put into our phones can be subject to government surveillance.273 Thankfully, the solution to this problem would not entail an overhaul of criminal procedure or investigations; rather, in the words of Chief Justice Roberts, the answer “is accordingly simple—get a warrant.”274

Sophie L. Nelson*

272. See Del Rosso & Bast, supra note 92, at 93.
273. See generally supra Part IV (discussing the Fourth Amendment and privacy implications in the current legal landscape).

* J.D. Candidate 2024, Pepperdine University Caruso School of Law; B.A. 2021, Pepperdine University Seaver College. Thank you to my family—Charlie, Stacey, Chase, and Peggy Nelson—for their unwavering support in my academic and personal endeavors. Thank you to Professor Shelley Ross Saxer for her guidance while drafting this Comment and to Professor Gregory S. McNeal for his specialized insight while refining this Comment. Thank you to the editors of Pepperdine Law Review Volumes L and LI for their support and helpful comments—I could not have been successful as an Editor-in-Chief and author without you all. Thank you to my beautiful law school friends for being a huge support system during the last three years (and beyond). Finally, thank you to Ryan Kenney for always encouraging me to shoot for the stars.