"Guarding the Sanctity of Choice and Privacy": Data Privacy and Abortion–The Next Frontier of the Fourth Amendment

Ryan S. Houser

Follow this and additional works at: https://scholarlycommons.law.northwestern.edu/njtip

Recommended Citation
https://scholarlycommons.law.northwestern.edu/njtip/vol21/iss2/2
“GUARDING THE SANCTITY OF CHOICE AND PRIVACY”: DATA PRIVACY AND ABORTION – THE NEXT FRONTIER OF THE FOURTH AMENDMENT

Ryan S. Houser
“GUARDING THE SANCTITY OF CHOICE AND PRIVACY”: DATA PRIVACY AND ABORTION – THE NEXT FRONTIER OF THE FOURTH AMENDMENT

Ryan S. Houser*

ABSTRACT—In the wake of the Dobbs decision, a seismic shift reverberates through the landscape of reproductive rights. As investigations into private healthcare decisions surge, states wield increasingly sophisticated tools to probe into the private lives of pregnant individuals, igniting a contentious debate on privacy and data security. The United States is entering a looming era where internet search histories, emails, text messages, and GPS data become ammunition in the arsenal of state-led investigations. Dubbed as “dragnet criminal surveillance tools,” these tactics will unleash a torrent of prosecutions, raising profound questions about the sanctity of personal information in the digital age. As the boundaries of privacy blur and the specter of Orwellian intrusion looms larger, the stage is set for a clash between legal precedent and technological innovation in the realm of reproductive justice.

This Article investigates the way in which recent court rulings and laws concerning data and privacy offer safeguards for forthcoming legal challenges post-Dobbs. With the proliferation of abortion inquiries due to state-level bans, the Fourth Amendment and Stored Communications Act offer vital protections against potential misuse of investigative methods, ensuring data and privacy rights are upheld.

This Article begins by analyzing the theoretical risks to data privacy and security post-Dobbs, illuminating potential issues through hypothetical scenarios and real-world examples. Additionally, this Article examines historical perspectives via pivotal court cases and policies on data privacy, contextualizing them within today’s landscape of protection. Ultimately, this Article, leveraging insights from both historical and contemporary viewpoints, contends that the current protective framework, grounded in

* Doctoral student, George Mason University – Schar School of Policy and Government. JD Rutgers Law School, MHA/MPH George Washington University Milken Institute School of Public Health, MSc/EMPS Georgetown University. The author extends grateful thanks to Professors Andrew Pak and Erez Liebermann for their unique Cybersecurity and Data Protection course which inspired this piece.
the Fourth Amendment and the Stored Communications Act, serves as a safeguard against Dobbs-related challenges, particularly concerning technology-driven infringements on abortion-related matters.

**INTRODUCTION**

In June 2022, the Supreme Court sent shockwaves through the United States with a landmark decision, *Dobbs v. Jackson Women’s Health Organization*,¹ which overruled both *Roe v. Wade*² and *Planned Parenthood v. Casey*.³ *Dobbs* considered the constitutionality of a 2018 Mississippi law called the “Gestational Age Act,” which prohibited all abortions, with few exceptions, after fifteen weeks’ gestational age. The Court, overruling precedent, held that the Constitution does not confer a right to abortion. This was one of the first instances in which the Supreme Court eliminated a previously held fundamental right.⁴ As a result, access to abortion services is now dictated by each state in their own capacities. The *Dobbs* decision made an already daunting and difficult task even more challenging for women seeking abortions. Before *Dobbs*, the courts prohibited states from passing outright bans before the viability of the fetus while allowing them to enact restrictive abortion policies, which made it difficult for women to obtain an abortion.⁵ The *Dobbs* decision expanded the states’ control even further by allowing them to ban abortion pre-viability. This led to the enactment of several varieties of abortion bans across the United States, some of which were passed right after the *Dobbs* ruling.⁶ A month after the ruling, twenty-six states had banned or restricted abortion or were on the verge of doing so. Twenty-two states banned

---

⁵ Id.
abortion before twenty-three weeks, including fourteen states that effectively banned all abortion (with some exceptions for the life of the mother, rape, and incest depending on the state). From a purely numerical perspective, the 14 states that outlaw abortion outright effect more than 24.1 million women of reproductive age. The 12 states that ban pre-viability abortion or that have pending litigation about their bans effect more than 12.2 million women. In total, this leaves twenty-six states and 36.3 million women of reproductive age (48.8 percent) impacted by post-Doob's legislation.

While the full extent of the holding is yet to be realized, the ramifications of the decision are already beginning to emerge, posing significant legal hurdles and consequences for women seeking abortion services, their families, and healthcare providers. Fertility treatments are even raising potential legal considerations as abortion bans across the nation attempt to define personhood. Several states have enacted what are commonly referred to as “personhood” laws, which acknowledge the start of life as the moment of conception. These laws impose legal responsibility on individuals who harm a fetus and subject them to criminal penalties. In addition, certain states have gone beyond this and incorporated the concept of fetal personhood throughout their legal codes. In a number of states across the country, women have been investigated, prosecuted, and jailed for pursuing abortions. Prohibited laws that were directed towards protecting a fetus by defining life at conception, are now allowed under Dobbs, the effect of which will be realized in the increased criminal investigations of women. These invasive investigations could cause embarrassment, financial burden, trauma, and other negative

---

8 Id. at 9.
9 Id.
11 Id.
12 Id.
consequences. As investigations increase, states’ use of sophisticated tools to pursue investigations of pregnant women will be a concern and may contribute to a rise in prosecutions. A variety of experts have predicted a state increase in the use of internet search histories, emails, text messages, testimony of providers, GPS data, and other “dragnet criminal surveillance tools” which will cause the “number of prosecutions [to] just rise very dramatically.” These investigative tools implicate a number of privacy and data concerns.

This paper examines how recent court decisions and legislation regarding data and privacy extend protections to cases and legal issues that will arise post-Dobbs. While abortion investigations will universally rise across the country as a result of state laws banning abortion, the Fourth Amendment and Stored Communications Act both provide data and privacy protections that inform and protect against abuses of investigative tools that might ensue. Part I of this paper analyzes the theoretical threats to data privacy and security that could arise following the Dobbs decision. These emerging concerns will be highlighted by looking at both hypothetical modern-day applications of the law and existing real-world situations that have already occurred. Part II of this paper will explore the historical perspectives through key court cases and policies on data protection and privacy as they relate to the current protection landscape. Applying the historical and current perspectives discussed in Parts I and II, the final section, Part III of this paper, will argue that the existing protective landscape, underpinned by the Fourth Amendment and the Stored Communications Act, acts as a shield to Dobbs related cases in the context of technology-based Orwellian intrusion on matters related to abortion.

I. CONCEPTUALIZING THE THREATS

Let’s imagine for a moment that you are a person of childbearing age with a uterus. You had been using a period tracking application on your phone. For any number of valid reasons, you decide that you want to terminate your pregnancy. You live in a state which restricts abortion – particularly, a state where telemedicine for abortion is illegal. Like many

other women across the country, the nearest abortion center is in another state and is not accessible due to distance and cost. Lacking options, you quickly Google “how to get abortion drugs.” You find a site like AidAccess,\(^\text{17}\) which conducts telemedicine appointments and arranges shipments of mifepristone and misoprostol (abortion-aiding medications) from abroad, but you continue to search on your phone and computer to find the best option.

Alternatively, imagine now that you had an abortion center near you. You search on Google for directions to the center and the center’s services. While visiting the center for your procedure, you access its Wi-Fi and utilize various apps, messaging, and other services on your phone while waiting.

In both these scenarios, you aren’t concerned since you did everything privately on your phone. But should you be? The short answer is yes. Each of these situations pose a risk, as the data that is collected on your devices contain sensitive information that law enforcement can use against you. Your phone and computers track every move that you make, including “the search history stored on your Google Chrome browser, your internet service provider’s record of incoming and outgoing requests, the financial details tracked by your payment processor, the emails you send, and more.”\(^\text{18}\) This problem is only more prevalent as cellphone usage increases. Today at least 81% of Americans own a mobile phone and many rely solely on them for their daily activities.\(^\text{19}\) Mobile phones “remain the most frequently used and most important digital source for investigation.”\(^\text{20}\) Many Americans “especially people of color and people with lower incomes, rely solely on their cellphones to connect to the internet,” making them more susceptible to these prosecutorial tactics.\(^\text{21}\) Even more concerning is the fact that many law enforcement searches are done against people’s will or at least without meaningful consent. These searches utilize mobile device forensic tools that allow law enforcement to “extract a full copy of data from a cellphone — all emails, texts, photos, locations, app


\(^{20}\) Id.

\(^{21}\) Id.
data, and more — which can then be programmatically searched.”

These mobile device forensic tools provide a “window into the soul.” Moreover, the physical cell phone itself is not the only concern – cloud data is considered to be “a virtual goldmine of potential evidence.”

Data is a necessary consequence of our information society. Experts have warned that “everything we do leaves a data shadow, and that shadow is under constant surveillance.” While most of the concern may be initially about direct government interference, there are also concerns with non-governmental actors such as technology corporations which process data on a mass scale.

The Dobbs decision has converted what was once an abstract privacy argument amongst policy experts into a concrete real-world problem that affects a large percentage of the United States population. Overnight, battles between abortion-banning states, technology companies, and citizens over the gathering of criminal evidence became a near certainty.

Technology companies have become major actors in the world of law enforcement and national security. The number of law enforcement requests for information from technology companies is staggering. Over six months in 2017, Facebook received 32,716 requests for information (covering 52,280 user accounts and including 19,393 search warrants and 7,632 subpoenas), Google received 16,823 requests (for 33,709 accounts), and Twitter received 2,111 requests (for 4,594

---

22 Id. See also Mobile Security and Forensics, NIST, https://csrc.nist.gov/Projects/Mobile-Security-and-Forensics/Mobile-Forensics [https://perma.cc/866U-RNGE]. (“When mobile devices are involved in a crime or other incident, forensic specialists require tools that allow the proper retrieval and speedy examination of information present on the device. A number of existing commercial off-the-shelf (COTS) and open-source products provide forensics specialists with such capabilities.”)


27 Id.


30 Requests for User Information, GOOGLE TRANSPARENCY REP., https://transparencyreport.google.com/user-data/overview?user_requests_report_period=series:requests,accounts;time:
These companies produced at least some information for nearly eighty percent of requests, turning technology companies into evidence gatherers for thousands of investigations. These new battles have tangible consequences for those seeking abortion-related services and technology as simple as fertility tracking applications on smart phones could have devastating impacts on the liberty of women across the country.

These abortion-related privacy and data threats are not just conceptual. There are a number of concerning cases in which citizens were prosecuted for abortion related offenses. As recently as this year, Lizelle Herrera was arrested and jailed after allegedly performing a self-induced abortion in Texas. She spent three days in jail before she obtained bail. In 2015, Kenlissa Jones was charged with murder after allegedly taking pills that terminated her pregnancy. Although the murder charge was eventually dismissed, this case highlights the post-Dobbs shift that has made prosecution on abortion matters more prevalent.

Recent examples of prosecutions have been even more worrisome as they involved data privacy considerations, laying the groundwork for future intrusions. For example, Jennie McCormack needed an abortion in 2010, but was unable to make the trip from her small town in Idaho to Salt Lake City, the closest abortion clinic. Unable to afford the expensive trip to Utah, McCormack asked her sister to purchase abortion pills over the internet instead and mail them to her, in Idaho. McCormack was arrested pursuant to a 1972 law making it illegal for a woman to induce her own abortion.

[32] See supra note 29 (85%); supra note 30 (81%); supra note 31 (77%).
[35] Id.
[37] Id.
pregnancy. In this case, prosecutors used private text messages between Patel and a friend about purchasing abortion medication as evidence. Patel was initially convicted in 2015 and sentenced to twenty years in prison, although her conviction was overturned on appeal. One of the most concerning cases is from 2017 in which Latice Fisher was criminally prosecuted in Mississippi after investigators searched her cell phone and found she searched for information about how to obtain an abortion. She was prosecuted even without direct evidence that she had actually taken abortion medication. Finally, in 2022, a 41-year-old woman was arrested and faced felony charges in Nebraska for allegedly helping her teenage daughter abort a pregnancy. Her arrest came after police uncovered private Facebook messages that implied she was helping her daughter get an abortion.

These cases highlight how law enforcement and prosecutors use technology against women seeking abortions. Nearly every day police access private messages “between people on Facebook, Instagram, any social media or messaging service you can think of” as “[w]arrants for online messages are a routine part of police investigation.” This is an emerging concern due to the “far-ranging nature of how we expect abortion investigations are going to go.” With Dobbs’ destruction of Roe, “it’s going to touch many more people’s lives in a way that maybe that they hadn’t thought about in the past.” Social media messages, emails sent through burner accounts, apps that track menstrual cycles, and geolocation data are “just a few examples of potentially incriminating digital footprints that confront people seeking abortions.”

39 See Ali, supra note 17.
41 Id.
42 Id.
44 Id.
45 Id. (quoting Andrew Crocker, a senior staff attorney with the Electronic Frontier Foundation).
46 Id.
protections exist for citizens, it is first critical to investigate how these data driven threats emerge in our society and how seemingly unimpactful actions could have a great influence on those seeking abortion services or even regular obstetric and gynecological care.

Even outside these examples pertaining to communications, cell phones also produce a lot of data by just the passive use of the device. Cell site location information (“CSLI”) includes the approximate location of where calls begin and end based on a connection to cell towers. This information has been used in January 6th cases, for example, to pinpoint the physical location of various suspects. Law enforcement agencies can use CSLI to track the location of parties who visit abortion clinics. Similar location data is created by Google. Turning on these services allows location tracking data to be transmitted between Google and other services, like YouTube, that seemingly do not require the storage of location data to function, but do still utilize the data to alter a user’s experience. Following Dobbs, Google created a new program to automatically delete the location data of users who visit “particularly personal” locations, such as “counseling centers, domestic violence shelters, abortion clinics, fertility centers, addiction treatment facilities, weight loss clinics, cosmetic surgery clinics, and others.” While users can disable location services, they make many programs (e.g., Google Search, Google Maps) more accurate. The sudden absence of data could also become evidence in court.

Geo-fencing is another major threat facing women seeking abortion care. Geo-fencing is the use of location data to target people in a given area. Massachusetts is the only state that banned geo-fencing. This came to be after a 2015 lawsuit in which a Boston technology company was barred from sending targeted ads on behalf of anti-choice clients. Law enforcement can seize on this technology to craft “geofence” warrants that seek location data for every user within an area over a span of time. Period trackers are another concern as millions of women use apps to track their cycles, and that data is often given to third-party companies, like Facebook and Google. Flo, for example, invites more than 100 million users to “enter intimate details about their bodies that they might not share even with their closest friends or family: the color and consistency of

48 Id.
49 Rosenberg, supra note 26.
50 Id.
51 Kalish, supra note 18.
vaginal discharge, the length of their periods, whether they had protected or unprotected sex, whether they feel frisky or have a low libido.” This level of detail helps women “keep track of and demystify the reproductive cycle from its most fertile days to its least.” Flo’s users found comfort in the company’s promise to keep data collected through its app confidential. In reality, the company passed on certain intimate health details of its users to marketing and analytics companies like Facebook and Google for three years. The Federal Trade Commission stated, “Flo’s data-sharing practices had allowed third-party companies to use that ‘personal health information expansively, including for advertising.’” This data had the potential to be used to find and prosecute abortion-seeking individuals. While it may be easy to delete the Flo application, it is much harder to delete the data it collected. As a result, Flo has left many users vulnerable to investigations, should law enforcement subpoena this supposedly “private” data.

These issues directly implicate real-world events. As noted previously, Latice Fisher is an example of how data can be leveraged in investigations. Fisher arrived at a Mississippi hospital after a miscarriage. She admitted during an earlier gynecological exam that she was pregnant, but never returned for an ultrasound, which drew suspicion from medical officials. Fisher voluntarily provided her phone to the police. Prosecutors then scraped her search history, which included searches for misoprostol. They used Fisher’s searches as evidence that she had intentionally “killed” her fetus.

Fisher’s case is a sobering forecast of what could happen if protections are not enacted to prevent law enforcement from utilizing mass extraction tools or getting access to cellphone data. These risks, however, should not only be a concern for those seeking abortion or obstetric and gynecological services. Every American is at risk of having their phone forensically searched by law enforcement making it practically inevitable that everyone with a cell phone will face digital self-incrimination at some point.

54 Id.
55 Id. (noting in Flo’s policy that they stated noting that “even as it might share some personal data with other companies, it would not disclose details about ‘cycles, pregnancy, symptoms notes and other information that is entered by you.’”)
56 Id.
57 Id.
58 Kalish, supra note 18.
59 Id.
II. HISTORICAL PERSPECTIVES AND CURRENT PROTECTIONS

While there are a variety of concerns that exist within the field of data protection and privacy, there are some protections that exist within the United States. There are a variety of legislative approaches that provide data privacy protections. The Stored Communications Act, 18 U.S.C. §§ 2701-2712 (“SCA”), for example, sets forth a system of statutory privacy rights for customers and subscribers of computer network service providers.60 The SCA “permits the Government to compel the disclosure of certain telecommunications records when it ‘offers specific and articulable facts showing that there are reasonable grounds to believe’ that the records sought ‘are relevant and material to an ongoing criminal investigation.’”61 The act seeks to “protect and regulate the privacy interests of network users with respect to government, network service providers, and the world at large.”62 There are three main elements of this process:

1. § 2701 prohibits unlawful access to certain stored communications; anyone who obtains, alters, or prevents authorized access to those communications is subject to criminal penalties
2. § 2702 regulates voluntary disclosure by network service providers of customer communications and records, both to government and nongovernment entities.
3. § 2703 creates a code of criminal procedure that federal and state law enforcement officers must follow to compel disclosure of stored communications from network service providers.63

The SCA offers varying degrees of legal protection depending on the perceived importance of the privacy interest involved.64 It also prohibits tech companies from disclosing information without a valid legal request.65

Other legislation such as Health Insurance Portability and Accountability Act (HIPAA), The Gramm-Leach-Bliley Act, Right to Financial Privacy Act, and Federal Trade Commission Act (FTCA) are data privacy protection measures, but are not the focus of this note.

---

62 JARRETT ET AL., supra note 60, at 115.
63 Id.
64 Id. at 116.
The case of *Carpenter v. United States* is one of the most crucial tests for Constitutional protections in the face of emerging technology. The *Carpenter* case involves the reasonable expectation of privacy test and subsequent protections under the Fourth Amendment. The Fourth Amendment protects the “right of the people to be secure in their persons, house, papers, and effects, against unreasonable searches and seizures.” In *Carpenter*, investigators obtained a defendant’s cell phone records after his accomplice to a string of store robberies confessed his involvement. Carpenter challenged the prosecution’s admission of his cell phone data. Carpenter’s CSLI included “12,898 location points cataloging Carpenter’s movements over 127 days—an average of 101 data points per day.” The Supreme Court granted certiorari following Carpenter being “convicted on all but one of the firearm counts and sentenced to more than 100 years in prison.” The Sixth Circuit held that Carpenter lacked a reasonable expectation of privacy since cell phone users voluntarily convey CSLI to carriers, and the resulting business records would therefore not be entitled to Fourth Amendment protections.

*Carpenter* is not the first case to consider the expansion of Constitutional protections in a technological age. Much of the privacy case law before *Katz v. United States* revolved around property rights. In *Olmstead v. United States*, the Court did not consider wiretapping a search or seizure since it did not violate property rights. *Katz*, however, was the turning point. The Supreme Court found that the Fourth Amendment protects *people* rather than places. Extension of this viewpoint suggests that what a person seeks to preserve as private, even in a public area, may receive Fourth Amendment protection. This case, and the concurrence, produced the phrase “reasonable expectation of privacy,” giving rise to the analytical framework used in future Fourth Amendment jurisprudence.

---

67 U.S. CONST. amend. IV.
68 Carpenter, 138 S. Ct. at 2209.
69 Id. at 2213 (citing United States v. Carpenter, 819 F.3d 880, 888 (2016)).
70 Id.
72 Olmstead v. United States, 277 U.S. 438 (1928).
74 Katz, 389 U.S. at 351.
75 Id. at 351–52.
76 See id. at 360 (Harlan, J., concurring) (“I join the opinion of the Court, which I read to hold only . . . that an enclosed telephone booth is an area where, like a home . . . and unlike a field . . . a
Privacy protections do not extend to all forms of data, however. Following *Katz*, courts analyzed the “expectation of privacy” language. In *United States v. Miller*, Justice Powell, explained that there is no “zone of interest” that is impacted by government investigations unless “the security a man relies upon when he places himself or his property within a constitutionally protected area.”\(^77\) The Court’s reasoning was that the bank records in contention were considered business records. It noted, “a depositor takes the risk, in revealing his affairs to another that the information will be conveyed by that person to the government.”\(^78\) The Court thus implemented the “third party doctrine.” The Fourth Amendment does not prohibit the government from gathering this information revealed to a third party, even if the initial party revealed the information with an assumption of confidence and a limited purpose of use.\(^79\)

*Smith v. Maryland* further upheld the third-party doctrine. The Court limited the doctrine, finding that a pen register addition to the phone of a suspect that would record numbers dialed could be used as evidence for an indictment.\(^80\) Justice Blackmun, writing for the Court, indicated that people cannot retain an expectation of privacy in the numbers they dial since they are conveyed to a phone company which maintains records for the purposes of billing.\(^81\) Recognizing the reasonable expectation claims in *Katz*, the court followed *Katz*’s two step analysis and found that “even if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not one that society is prepared to recognize as reasonable.”\(^82\)

Knowing this, *Carpenter* was one of the first to grapple with the drastic implications of emerging technologies. The Court analyzed whether a warrantless search and seizure of cell phone records which included location and movements of phone users violated the Fourth Amendment. A 5-4 majority held that the government’s warrantless “acquisition of the cell-site records was a search within the meaning of the Fourth Amendment.”\(^83\) The reasonable expectation of privacy standard influenced the case, as the majority held that “individuals have a reasonable

---

78 Id. at 443.
79 Id.
81 Id. at 742.
82 Id. at 743 (internal quotation marks omitted).
83 Carpenter, 138 S. Ct. at 2220.
expectation of privacy in the whole of their physical movements.”

Recognizing a “chronicle of a person’s physical presence compiled every day, every moment, over several years” to be a privacy concern extending “far beyond those considered in Smith and Miller,” the Courts extended the Fourth Amendment’s protections. The Court found the voluntary exposure rationale underlying the third-party doctrine to be invalid as related to CSLI. The majority noted that a “cell phone logs a cell-site record without any affirmative act on the part of the user beyond powering it up.” Any activity on a phone generates CSLI, even those that are outside the traditional calls and messaging.

The most recent case to consider the Fourth Amendment protections related to phone-created data is Chatrie. The case stemmed from a 2019 Virginia bank robbery. Law enforcement investigating the case had no leads for the suspect. Law enforcement did know, however, that the suspect had a cellphone with him based on the bank teller’s comments. Police then obtained a geofence warrant from a state magistrate judge. The warrant sought to identify “each phone logged into Google within a 150-meter radius of the bank from 30 minutes before the robbery to 30 minutes after the robbery.” Following the signature of the warrant, Google informed law enforcement that nineteen phones were responsive to the warrant. The production from Google “revealed the location patterns of the nineteen phones during the hour window, showing the area the phones were thought to be in, and when, over the hour.” The government then requested “the actual identity of three of the phone owners according to Google’s records, reflecting the phones that investigators believed, based on the patterns of location over the two hours, were the bank robber and possible co-conspirators in the area.” Law enforcement identified Chatrie and he moved to suppress the evidence. The court found that the “analysis of geo-fences does not fit neatly within the Supreme Court’s existing ‘reasonable expectation of privacy’ doctrine as it relates to technology. That run of cases primarily deals with deep, but perhaps not wide,

84 Id. at 2217 (citing United States v. Jones, 565 U.S. 400, 430 (2012)).
85 Id. at 2220.
86 Id.
87 Id.
89 Id.
90 Id.
intrusions into privacy.”92 The court concluded that the warrant “plainly” violated the Fourth amendment but applied a good faith exception after determining that “reliance on the Geofence Warrant was [not] objectively unreasonable.”93

III. THE SHIELD AGAINST ORWELLIAN SURVEILLANCE

Given the threats to the health, safety, and justice of women across the country, the legal landscape that protects against the government’s improper access of private data has elevated importance. The legal landscape around data privacy in the post-Dobbs era is unclear. The last Supreme Court case on matters related to these threats was Carpenter, which leaves an avenue for continued Fourth Amendment protection. However, the Carpenter majority found that their ruling was “a narrow one” that does not “express a view on matters not before” the Court.94 The holding in the Chatrie case could similarly be an important precedent regarding data privacy. The case has not been appealed for a ruling by an appeals Court or Supreme Court which calls into question the concreteness of its protections. Additionally, the SCA’s protections depend on the perceived importance of the privacy interest involved.95

Without recent case law, it is critical that we consider Carpenter in light of the potential post-Dobbs privacy threats. The Carpenter majority extended the Fourth Amendment doctrine within the ‘reasonable expectation of privacy framework’ to ensure that legislation adapts to the modern technological landscape. While the dissent relied on the history of the Fourth Amendment and a property-based approach, utilizing this approach to privacy is futile as it eliminates the previously created expectations of privacy which have been expanded to reflect our digital age. The extension of the reasonable expectation of privacy test ensures protection against intrusive searches, including tracking a person’s every location through a cellular device. This doctrinal extension is necessary, as no legislature or court could have anticipated such an advancement in technology.

The Court’s refusal to apply the third-party doctrine to CSLI has broader implications. A failure to consider the words of the Court in similar

92 Chatrie, 590 F. Supp. 3d at 926. See, e.g., Kyllo v. United States, 533 U.S. 27, 34 (2001) (considering the validity of using thermal imaging on one’s home); United States v. Jones, 565 U.S. 400, 402-03 (2012) (construing “the attachment of a [GPS] tracking device to an individual’s vehicle” for twenty-eight days); Carpenter, 138 S. Ct. at 2217 n.3 (considering whether “accessing seven days of [an individual’s cell site location information] constitutes a Fourth Amendment search”).
93 Chatrie, 590 F. Supp. 3d. at 905, 941.
94 Carpenter, 138 S. Ct. at 2220.
95 Id. at 2215.
contexts is a logically flawed approach. Distinguishing the facts of Carpenter from Smith and Miller, the Court did not rely solely on the act of sharing and instead “considered ‘the nature of the particular documents sought’ to determine whether ‘there is a legitimate ‘expectation of privacy’ concerning their contents.’”96 This statement is one of the most protective. As discussed by the Court, CSLI is an increasingly precise personal GPS data generator.97 Cell phones constantly communicate with the nearest cell tower.98 Through this data, without any reasonable protections, the government can recreate the movements of a cell phone user at every moment of the day.99 The same implications exist for geo-fencing and Google. The claim that warrants should be permissible to acquire such data based on the voluntary principle is incorrect.

There are proponents who argue that all data a user provides is voluntary. Their argument posits that users do not have to agree to share location data and can turn their phone off or on “airplane mode” when they do not want to be tracked. Similar consent arguments are made for network service providers under the SCA, where there is an argument that “[t]erms of service used by network service providers often establish that the provider has authority to access and disclose subscriber email.”100 For example in United States v. Young, Yahoo!’s terms of service confirmed its right in its “sole discretion to pre-screen, refuse, or remove any Content that is available via the Yahoo! Services,” as well as to access and disclose email to comply with legal process.”101 These corporate terms of service were sufficient to establish Federal Express’s common authority over the contents of a package in this case.102

These arguments ignore the reality of the necessity of technology today. In Carpenter, the Court stated that “cell phones and the services they provide are ‘such a pervasive and insistent part of daily life’ that carrying one is indispensable to a participation in modern society.”103 Users have no remedies for avoiding leaving a trail of data other than “disconnecting the

---

96 Carpenter, 138 S. Ct. at 2219 (citing United States v. Miller, 425 U.S. 435, 442 (1976)).
98 See Carpenter, 138 S. Ct. at 2206.
99 Ricciuti, supra note 97, at 406.
100 JARRETT ET AL., supra note 60, at 146.
101 Id.
102 United States v. Young, 350 F.3d 1302, 1308–09 (11th Cir. 2003) (holding that Federal Express’s terms of service, which authorized it to inspect packages, gave it common authority to consent to a government search of a package). See generally Warshak v. United States, 532 F.3d 521, 527 (6th Cir. 2008) (en banc) (noting the range of terms of service used by different providers).
103 Carpenter, 138 S. Ct. at 2220 (citing Riley v. California, 573 U.S. 373 (2014)).
phone from the network.”  

This is an impossible task for users as they attempt to navigate in the technology-tethered everyday world that we live in. This reality limits today’s technology sharing to only faux-voluntary submission of data based on social pressures and the advances within the technology. The prevalence and necessity of technology effectively defeats any notion of the volitional submission of data. In order to purchase and use a cellphone, parties must “agree to legal terms and conditions, ranging from the cell phone provider and manufacturer to an app creator.” Users often ignore these terms and conditions – in fact, “91% of users “accept legal terms and conditions without reading them before installing apps, registering Wi-Fi hotspots, accepting updates, and signing on to online services such as video streaming.” Even for the small number who do read the terms and conditions, the “vast majority of terms and conditions are too complex for many people to understand.” The policy considerations behind leaving a large majority of the population completely vulnerable to intrusion on reasonable expectations of privacy, with no ability to provide informed consent with regards to the data they are sharing, is absurd. This is even in addition to the inability based on societal necessity to opt out of sharing data in order to maintain privacy. Evidently, it is highly unlikely that most of the population is aware of the amount of data that they are sharing through their phone and other services.

The Fourth Amendment protections in Carpenter extend to other threats such as third-party applications, including period-tracking applications, or internet searches. In Carpenter, Justice Sotomayor remarked, “it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.” Finding that the third-party doctrine is “ill-suited to the digital age,” Justice Sotomayor’s statements suggest that the Court is willing to accept a broader protection of privacy expectations. Even Justice Gorsuch voiced similar concerns in Carpenter, questioning whether the government could “demand a copy of all your e-mails from Google or Microsoft without implicating your Fourth Amendment

104 Id.


106 Id.

107 Id.


109 Id.
Justice Gorsuch also extended the question to DNA platforms like 23andMe where without a warrant or probable cause, the government could demand access, “at least without running afoul of Katz.” A finding that would trouble almost all Americans. Allowing such a result “strikes most lawyers and judges today “as pretty unlikely.” Asking parties to turn off their phones to avoid Google searches or Wi-Fi access to avoid providing unintentional data is infeasible. The ability of the government then to leverage data shared to third-party apps with the expectation of privacy, such as CSLI under SCA § 2703(d), IP addressed from parties who are at clinics under § 2703(c)(2), or Google location history services (Geofence warrants) and reverse search history warrants, is thus a wholly improper violation of the principles of the Fourth Amendment. Such data is not without its problems, however. Google Data, for example, led to a wrongful arrest for murder. The law should, therefore, protect American citizens from the government’s unconstitutional intrusions. This is, and has always been, the goal of the Fourth Amendment. Any deviation does not conform to the ideals of the country.

All of this is not to say that these theoretical protections are perfect. Although the Supreme Court in Riley v. California, 573 U.S. 373 (2014), held that in order to search a phone, police had to have a warrant, consent searches have “long been understood to be an exception to the Fourth Amendment’s warrant requirement.” Research found that a good portion of phone searches were consensual. While obtaining consent may be an appropriate method, the general public’s limited knowledge of the data on their devices makes their consent uninformed. The Fourth Amendment also requires that law enforcement describe with particularity the places being searched and the items being seized. This particularity requirement intends to protect citizens from general warrants such that law enforcement

---

110 Carpenter v. United States, 138 S. Ct. 2206, 2262 (Gorsuch, J., dissenting).
111 Id.
112 Id.
114 Koepke et al., supra note 19.
115 See Koepke et al., supra note 19 (finding that 53% of Harris County (TX) Sheriff’s Office search of phones were consent searches or searches of phones that were “abandoned/deceased” and only nearly half of Denver Police Department phones searched were pursuant to a search warrant).
116 U.S. CONST. amend. IV (“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” (Emphasis added)).
cannot indiscriminately rummage through a person’s property. Some law enforcement agencies do not support these ideals. The Illinois State Police, for example, encourage broad search warrants, noting that “[a]ll computer hardware and software should be included [in search warrant applications], keeping in mind the entire system is necessary to replicate the suspect’s use of it and to enable forensic examination of the system.”\textsuperscript{117} The Indianapolis Metropolitan Police Department even goes as far as directing officers to request forensic analysis to describe “the evidence you expect to recover from the exam. Be specific as to what information the examiner should search for, such as ‘Evidence of Dealing Narcotics’ . . . [d]on’t list types of data (e.g. call log, text, email, etc. . . .) as your search warrant should cover all data.”\textsuperscript{118} The risk of overly broad searches is concerning because it violates the intentions of the Fourth Amendment and is nearly “impossible for those outside of law enforcement — such as a defense lawyer — to repeat the steps that a forensic examiner took and to audit the scope of a search.”\textsuperscript{119} Additionally under the SCA, “even if a user has a reasonable expectation of privacy in an item, a subpoena may be used to compel the production of the item, provided the subpoena is reasonable.”\textsuperscript{120} As noted by Justice Alito in his dissent, some of the extensions offered by \textit{Carpenter} are “revolutionary” and a “departure from the “original understanding of the Fourth Amendment and more than a century of Supreme Court precedent” \textsuperscript{121} as noted by Justice Alito in his dissent, a departure that mimics the later radical departure of precedent in the \textit{Dobbs} decision. The departure in the \textit{Carpenter} case, however, is a necessary revolution to extend the principles foundational to our Constitution to an evolving landscape that was not imagined at the time of drafting.

Justice Alito further argued that \textit{Carpenter} would “encourage the public to think that the Court can protect them from this looming threat to their privacy.”\textsuperscript{122} This seems a valid and reasonable expectation, as the Court would be upholding the principles of the Fourth Amendment. Cell phones, “could just as easily be called cameras, video players, rolodexes,
calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.\textsuperscript{123} It is unlikely that the court would be comfortable allowing government intrusion into calendars, libraries, or albums that would even fall within the traditional context of “papers.” As technology continues to advance, we will continue to become further connected with digital systems which track our every movement and action out of necessity. The extension of the Fourth Amendment to protect from unreasonable access to this information is a necessary shield from improper governmental intrusion.

The overturning of \textit{Roe v. Wade} sparked an urgency to improve the technologies and legal system on which we depend. The Constitutional right to privacy in a broad context is eroding, but recent rulings of the Court suggest a recognition of historic property rights. While the \textit{Dobbs} decision enhances the potential implications of data protection and privacy as healthcare related procedures are now fragmentedly illegal throughout the United States, the protections to ensure data privacy already exists under the mighty pillar of the Fourth Amendment.

\textsuperscript{123} Riley v. California, 573 U.S. 373, 393 (2014).