My Health Data Was Sold to Who?: Louisiana's Lack of Privacy Protections for Sensitive Health Information Shared with Health Tracking Apps

Katherine Labadie*

* © 2025 Katherine Labadie, Managing Editor, *Tulane Journal of Technology and Intellectual Property* Volume 27, J.D. 2025, Tulane University Law School; B.A. 2019, Liberal Arts, Sarah Lawrence College. The author thanks the *Tulane Journal of Technology and Intellectual Property* editors for their support throughout the writing and editing of this Comment.

I. INTRODUCTION

Feminine technology ("FemTech") companies first launched period tracking apps, which log menstrual cycle information, in 2013 to help women monitor and manage their reproductive health and wellness.[1] These period tracking apps quickly gained popularity among consumers, with one app reaching 50 million users worldwide by 2020.[2] When the U.S. Supreme Court overturned *Roe v. Wade* with the *Dobbs* decision in 2022, privacy concerns regarding the sensitive health information logged on these period tracking apps escalated, particularly regarding whether this information could be subpoenaed and used to prosecute women for obtaining abortions.

Period tracking apps are marketed as useful tools for individuals trying to conceive, prevent pregnancy, or monitor health issues related to the menstrual cycle.[3] When these apps were first released, FemTech companies promoted the idea that they could collect data to enhance the field of women's health. The FemTech companies even hinted at future

1. Lauren Worsfold, et al., *Period Tracker Applications: What Menstrual Cycle Information Are They Giving Women?*, NATIONAL LIBRARY OF MEDICINE (Oct. 9 2021), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8504278/ (citing Bob Kronemeyer, *Female Health Technology Takes Center Stage*, CONTEMPORARY OB/GYN (Oct. 22, 2018), https://www.contemporaryobgyn.net/view/female-health-technology-takes-center-stage. ("The term 'FemTech' was coined by Ida Tin, the co-founder and CEO of the period tracking app, Clue.").

2. *Id.* (citing Donna Rosato, *What Your Period Tracker App Knows About You*, CONSUMER REPORTS (updated Jan. 28, 2020), https://www.consumerreports.org/health/health-privacy/what-your-period-tracker-app-knows-about-you-a8701683935/).

3. *See* Donna Rosato, *What Your Period Tracker App Knows About You*, CONSUMER REPORTS (updated Jan. 28, 2020), https://www.consumerreports.org/health/health-privacy/what-your-period-tracker-app-knows-about-you-a8701683935/ ("Depending on the app, that can include how often you have sex, if you are trying to have a baby, and whether you engage in unprotected sex, have experienced a miscarriage, or are approaching menopause."); *see also* Worsfold *supra* note 1. The apps allow women to track their menstrual cycles and receive predictions for the start of their future cycles, the day of ovulation, and the fertile window. Some period tracking apps use self-learning algorithms to improve cycle predictions, others base their predictions on the average twenty-eight-day cycle.

partnerships with healthcare providers.[4] While the implications for advancing women's health research were significant, data privacy experts cautioned against sharing deeply personal health information with applications not protected by HIPAA.[5]

Then, in the aftermath of the *Dobbs* decision that overturned *Roe v. Wade* and immediately criminalized abortion in states with relevant trigger laws, consumers were once again urgently warned to consider deleting their period tracking apps.[6] Now, sensitive health information collected by these apps can be shared not only with third-party holders and advertisers but also potentially with law enforcement in connection with criminal investigations of illegal abortions.[7] From there, this sensitive health data could be used as evidence that a person was pregnant before an alleged abortion.[8]

While the lack of privacy in data collected by health tracking apps has implications for insurance coverage and employment screenings, this Comment specifically examines the digital privacy laws in Louisiana in

4. Bob Kronemeyer, *Female Health Technology Takes Center Stage*, CONTEMPORARY OB/GYN (Oct. 22, 2018), https://www.contemporaryobgyn.net/view/female-health-technology-takes-center-stage. (Paljit Sohal, principal consultant at Frost & Sullivan, discussed the potential for health care companies to acquire FemTech apps or partner with specialized FemTech companies).

5. *See generally* Rosato, *supra* note 3; Kaitlyn Tiffany, *Period Tracking Apps Are Not for Women*, VOX (updated Nov. 16, 2018), https://www.vox.com/the-goods/2018/11/13/18079458/menstrual-tracking-surveillance-glow-clue-apple-health; Alisha Gupta & Natasha Singer, *Your App Knows You Got Your Period. Guess Who It Told?*, N.Y. TIMES (Jan. 28, 2021), https://www.nytimes.com/2021/01/28/us/period-apps-health-technology-women-privacy.html.

6. *See generally*, Catherine Roberts, *These Period Tracker Apps Say They Put Privacy First. Here's What We Found.*, CONSUMER REPORTS, https://www.consumerreports.org/health/health-privacy/period-tracker-apps-privacy-a2278134145/#:~:text=In%20general%2C%20whether%20using%20period,%2C%20companies%2C%20or%20law%20enforcement. (last updated Aug. 30, 2022); *Tech and Reproductive Rights*, AMNESTY INTERNATIONAL, https://www.amnestyusa.org/issues/technology/tech-and-repro/#:~:text=The%20FTC%20alleges%20that%20the,seekers%20and%20activists%20at%20risk (last updated Feb. 9, 2024); Kashmir Hill, *Why Deleting Your Period Tracker Won't Protect Your Privacy*, N.Y. TIMES (July 1, 2022), https://www.nytimes.com/2022/06/30/technology/period-tracker-privacy-abortion.html; Betsy Reed, *Why US Women are Deleting Their Period Tracking Apps*, THE GUARDIAN (June 28, 2022), https://www.nytimes.com/2022/06/30/technology/period-tracker-privacy-abortion.html; Nicole Wetsman, *How To Delete Your Period Tracking App Data*, THE VERGE (June 30, 2022), https://www.nytimes.com/2022/06/30/technology/period-tracker-privacy-abortion.html; Sara Morison, *Should I Delete My Period Tracking App? And Other Post-Roe Privacy Questions*, VOX (July 6, 2022), https://www.vox.com/recode/2022/7/6/23196809/period-apps-roe-dobbs-data-privacy-abortion.

7. *Id.*

8. *Id.*

relation to the state's criminalization of abortion.[9] First, the Comment provides an overview of the period tracking apps available on the market, analyzing the scope of the information they collect and the claims they make about data protection compared to the actual privacy afforded to that health data. Next, the existing framework in the United States for health information and online data privacy is discussed, highlighting how these laws fail to encompass protections for the sensitive information collected by health tracking apps. Both federal and state privacy laws are considered, along with proposed federal and state data privacy legislation. Finally, the status of data and health information privacy in Louisiana is addressed, concluding with proposals for amendments to Louisiana's current privacy laws that would extend protection to the types of sensitive health information collected by period and other health tracking applications.

II. PERIOD TRACKING APPS: AN OVERVIEW

The five most downloaded period tracking apps in the United States in 2022 were Flo, Clue, Stardust, Period Calendar, and Period Tracker.[10] All five apps store user data on a cloud, share user information with third parties, retain deleted user data for limited durations of time, and use location tracking.[11] Such decisions jeopardize the privacy of users' sensitive health information, even though period tracking apps tout their commitment to keeping user data secure.[12]

A. Cloud-Based Systems, Data Retention, and Location Tracking Pose Security Risks to Sensitive Health Information

1. Cloud Data

Most popular apps store user data in cloud-based systems.[13] A cloud-based system is a network of remote servers that operate as a single

9. *See further*, Alexis Guadarrama, *Mind the Gap: Addressing Gaps in HIPAA Coverage in Mobile Health Apps Industry*, 55 HOUS. L. REV. 999 (2018).

10. 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/?redirectURL=https://www.wired.com/story/period-tracking-apps-flo-clue-stardust-ranked-data-privacy/ APPMAGIC, https://appmagic.rocks/top-charts/apps?date=2024-01-01&aggregation=year&tag=243520&country=US).

11. *Id.*

12. *Id.*

13. *Id.*

ecosystem.[14] Essentially, health tracking apps store user data across multiple servers in different locations. The use of cloud storage allows apps to process large amounts of information for data recovery, but it can also make user data more vulnerable to bad actors.[15]

User data is more vulnerable in cloud-based systems because cloud users often have no way of knowing the precise location of their outsourced data within the cloud storage.[16] Therefore, the potential for internal or external malicious attacks presents a significant security challenge for sensitive health information, as these attacks jeopardize data integrity and confidentiality.[17] With malicious cloud storage providers, a lack of transparency regarding access to and control of data could result in the disclosure of confidential or sensitive information to others for business profit.[18] With external attacks, sensitive data could be lost, modified, or damaged.[19]

Privacy data experts recommend mobile health apps that allow users to store information directly on their devices rather than on a cloud-based system.[20] They explain that if an app stores data directly on a user's cell phone, the user will have more control over the data, making it less vulnerable to bad actors.[21] None of the five most popular period tracking apps offers users the option to store their data directly on their cell phones, but newer apps like Drip, Euki, and Periodical allow for local data storage.[22]

2. Data Retention

When period tracking apps store data in cloud-based systems, users' sensitive health information can remain accessible to the app company and third parties.[23] Simply deleting the apps does not delete user data. Users must deactivate their accounts to delete their data, and even then,

14. *What Is the Cloud?*, MICROSOFT AZURE, https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-the-cloud.

15. *Id.*

16. Paromita Goswami, *Investigation on Storage Level Data Integrity Strategies in Cloud Computing: Classification, Security Obstructions, Challenges and Vulnerability*, 13 J. OF CLOUD COMPUTING 727, 731 (2024).

17. *Id.*

18. *Id.*

19. *Id.*

20. *See* Poli, *supra* note 10.

21. *Id.*

22. *Id.*; Roberts, *supra* note 6.

23. Wetsman, *supra* note 6.

period tracking apps may take several weeks to comply with the deletion process.[24]

For example, the period tracking app Flo retains user data for up to three years after the app is deleted, in case users reactivate their account.[25] Flo does note that users can contact them to have their data deleted earlier; however, if users do not take this extra step, their data is able to be shared by the Flo app in response to subpoenas, court orders, or legal processes.[26]

The five most popular period tracking apps provide users with different levels of control over when and how thoroughly their data is deleted, but none offers the right to a total data deletion.[27] Period tracking apps that allow users to store their data locally do not require a data deletion policy, as the user data resides on individual devices, so the apps do not need to delete the data on behalf of users.[28]

3. Location Tracking

Some period tracking apps not only collect sensitive health information but also users' location data.[29] The location data collected by these apps and shared with third parties could find its way into legal proceedings through geofence warrants.[30] To obtain a geofence warrant, police must specify a location and time period during which a crime occurred, and then companies are required to hand over user's location data, unless the warrant is successfully challenged in court.[31] There is concern that subpoenas and geofence warrants could be used to obtain data indicating that a period tracking app user was pregnant and/or visited an abortion clinic.[32]

---

24. *Id.*; *see also Deleting Your Period Tracker Won't Keep Your Health Data Private*, JOHN HOPKINS INFO. SECURITY INST. (July 19, 2022), https://isi.jhu.edu/2022/07/19/deleting-your-period-tracker-wont-keep-your-health-data-private/ (the ability to delete health tracking apps lulls users into a false sense of security because the phone itself, individual apps, and web browsers can maintain a significant amount of data even when apps are deleted).

25. *Id.* (citing *Privacy Policy*, FLO (updated Oct. 31, 2023) ("you can still ask for your data to be deleted at an earlier date by contacting us") https://flo.health/privacy-policy#:~:text=Retention%20of%20your%20Personal%20Data&text=Impact%20of%20Account%20Deactivation%2FRequests,emailing%20support%40flo.health).

26. FLO, *supra* note 25.

27. Roberts, *supra* note 6.

28. *Id.*

29. Roberts, *supra* note 6.

30. *Id.*

31. *Id.* (*citing Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508).

32. *See id.*

There is currently no federal standard regulating the collection, use, or disclosure of geofence technology data in the United States.[33] All of the five most popular period tracking apps use location tracking. Three of the five—Flo, Clue, and Stardust—may also send users' IP addresses to third parties.[34]

B. Extent of Voluntary Disclosure to Third Parties

Health and period tracking apps typically share user data with third parties for marketing, research, and improving developer services.[35] For example, Period Tracker's privacy policy states that users' device IDs may be shared with advertisers and that, in the event of a corporate merger or sale, Period Tracker may sell or transfer user data.[36] Even Stardust, a period tracking app committed to limiting information shared with third parties, states in its privacy policy that it could share information to comply with or respond to law enforcement.[37]

While period apps that share user data with third-party research groups typically anonymize users' sensitive health information, it is challenging to anonymize anything completely.[38] Under certain conditions, anonymized data can still lead back to individual users.[39] This "re-identification" process has only been accelerated by machine learning.[40]

---

33. *USA: New Geofence Technology Laws*, ONETRUST DATAGUIDANCE REGULATORY RESEARCH SOFTWARE, https://www.dataguidance.com/opinion/usa-new-geofence-technology-laws#:~:text=Currently%2C%20no%20federal%20standard%20exists,Connecticut%20%E2%80%93%20enacted%20geofence%20technology%20laws.

34. *See supra* note 10.

35. *See also* JOHN HOPKINS INFORMATION SECURITY INSTITUTE, *supra* note 24. ("The whole model for apps has been to harvest as much data as possible in order to use that data for different purposes, including marketing.").

36. Kristen Poli, *The Most Popular Period-Tracking App Ranked by Data Privacy*, WIRED (July 28, 2022), https://www.wired.com/story/period-tracking-apps-flo-clue-stardust-ranked-data-privacy/?redirectURL=https://www.wired.com/story/period-tracking-apps-flo-clue-stardust-ranked-data-privacy/.

37. *Id.*

38. *Id.*; *see also supra* note 27.

39. Poli, *The Most Popular Period-Tracking App Ranked by Data Privacy*, *supra* note 36; *see further*, *This Algorithm can Identify 99.98% of American 'Anonymized' Datasets*, TECH MONITOR (updated July 25, 2019), https://techmonitor.ai/technology/data/de-anonymized-researchers.

40. *Id.*

C. Disclosure to Consumers—Flo's Settlement with the FTC

Period tracking apps generally lack adequate privacy protections and have a history of misleading consumers about data privacy.[41] In 2021, the period tracking app Flo entered into a settlement agreement with the Federal Trade Commission (FTC) for allegations that the app shared sensitive health information with outside companies after promising consumers that their data would remain private.[42]

The FTC's complaint alleged that Flo disclosed health data from millions of users of its Flo Period Ovulation Tracker app to third parties that provided marketing and analytic services to the app, including the analytics divisions at Facebook (Meta) and Google.[43] Despite the disclosed health data including sensitive information, such as pregnancy status, Flo did not restrict how third parties could use this health data.[44]

The sharing of this sensitive health information was not prohibited per se, but in sharing such health data without adequate notice and choice to users, they violated the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks.[45] Flo violated Privacy Shield principals no. 1, 2, 3, and 5 by failing to provide adequate notice for third-party use of health information for advertising and other purposes; failing to provide adequate choice for third-party use of health information for advertising, product improvement, and other purposes; failing to provide accountability for

41. Nicole Wetsman, *Flo Period Tracker Launches Anonymous Mode to Fight Abortion Privacy Concerns*, THE VERGE (Sept. 14, 2022), https://www.ftc.gov/news-events/news/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc-allegations-it-misled-consumers-about.

42. *Id.* (*citing* FTC report); In the Matter of Flo Health, Inc. Complaint, 1 (June 22, 2021), https://www.ftc.gov/system/files/documents/cases/192_3133_flo_health_complaint.pdf. ("These users trust Respondent with intimate details of their reproductive health because Respondent repeatedly promised to protect the information and keep it secret. Indeed, Respondent's privacy policies stated, time and again, that Respondent would not share users' health details with anyone.").

43. *Developer of Popular Women's Fertility-Tracking App Settles FTC Allegations that It Mislead Consumers About the Disclosure of their Health Data*, FED. TRADE COMM'N (Jan. 13, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc-allegations-it-misled-consumers-about.

44. *Id.*

45. The Flo app has been a member of the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks since 2018. To join the Privacy Shield Frameworks, companies must self-certify to Department of Commerce and publicly declare that they fully comply with the Frameworks' "Privacy Shield Principles." Companies under the jurisdiction of the FTC, such as Flo, are subject to the enforcement of the Privacy Shield Principles under section 5 of the Federal Trade Commission Act. *Id*; In the Matter of Flo Health, Inc. Complaint, *supra* note 42 at 10.; *see further* EU-U.S. and Swiss-U.S. Privacy Shield Frameworks at 5.

onward transfers of user data; and failing to process personal information in a way that is compatible with the purposes for which it has been authorized by the individual users.[46]

The settlement agreement between Flo and the FTC required Flo to obtain an independent compliance review of its privacy practices and to get app users' consent before sharing their health information.[47] The independent compliance review had to (1) determine whether Flo maintained compliance with the EU-U.S. and Swiss-U.S. Privacy Shield Principles, (2) assess whether Flo's privacy practices were consistent with its privacy policy, (3) evaluate whether Flo adequately informed individuals about the mechanisms through which they may pursue privacy practice complaints, (4) identify any gaps or weaknesses in the privacy practices assessed, and (5) provide specific evidence examined to support such determinations and explain why the evidence was sufficient to justify the findings.[48]

The provisions of the settlement also established specific requirements for the Flo app to comply with going forward. First, the settlement prohibited Flo from misrepresenting their information privacy and data deletion policies.[49] Second, the provisions required Flo to instruct any third party that received user health information from Flo to destroy such information.[50] Third, Flo was required to disclose the nature of the user data given to third parties and the names of those third parties to existing users.[51] Finally, Flo was required to clearly and conspicuously disclose their updated privacy policy and terms of use to new and existing users and obtain affirmative express consent to the policy and terms from these users.[52]

Nevertheless, an ongoing concern among data privacy experts is that users agree to the privacy policies of health and period tracking apps before they can use the app and while being fully aware of the extent of

46. In the Matter of Flo Health, Inc. Complaint, *supra* note 42 at 7-9.

47. *Id.* at 5.; *see further* FTC Proposed Settlement Agreement with Flo Health, Inc., FED. TRADE COMM'N, 5, (Jan. 13, 2021), https://www.ftc.gov/system/files/documents/cases/flo_health_order.pdf.

48. In the Matter of Flo Health, Inc., Decision and Order 5, (June 22, 2021), https://www.ftc.gov/system/files/documents/cases/192_3133_flo_health_decision_and_order.pdf (evidence examined included documents reviewed, sampling and technical testing performed, and interviews conducted).

49. *Id.* at 3, 4.

50. *Id.* at 4.

51. *Id.*

52. *Id.*

the sensitive health data that is collected and disclosed to third parties.[53] Furthermore, although claims made in privacy policies are enforceable under the Federal Trade Commission Act, health-related information collected by apps is not inherently protected by any significant privacy law, including the Health Insurance Portability and Accountability Act (HIPAA).[54]

III. PRIVACY LAW REGULATING REPRODUCTIVE HEALTH DATA

A. HIPAA Limitations

Health data is protected only in limited circumstances. HIPAA states that health care professionals and insurers cannot use or disclose health records and protected health information without a patient's express consent.[55] However, HIPAA provisions typically do not extend to sensitive health data gathered in nonmedical settings.[56] The level of protection for health data depends on where it is held, rather than the nature of the data.

Under HIPAA, mobile health apps linked to "covered entities" receive robust protections. Covered entities include health plans, health care clearinghouses, and health care providers who transmit health information electronically. Crucial to mobile health apps, HIPAA also applies to business associates of covered entities.[57] Therefore, user data collected by mobile health apps connected with covered entities is subject to HIPAA protections. By contrast, mobile health apps that collect the same or similar sensitive health information, but are not associated with a covered entity, are not only left without HIPAA protections; they are also left essentially unregulated.

Most period tracking apps do not connect with covered entities, meaning they are not subject to HIPAA regulations. None of the top five most downloaded period tracking apps falls under HIPAA regulation.[58]

---

53. Poli, *The Most Popular Period-Tracking Apps, Ranked by Data Privacy, supra* note 10.

54. *Id.*

55. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.

56. In some cases, medical providers might disclose protected health information to law enforcement without patient consent. Guadarrama, *supra* note 9 at 1004.

57. Common business associates under HIPAA to include third-party administrators helping a health plan with claims processing, consultants who perform utilizations reviews for hospitals, and independent medical transcriptionists who provide transcription services to physicians. 45 C.F.R. § 160.103 (2016).

58. Erin Jones, *No, Health Data from Most Period-Tracking Apps Is Not Protected Under HIPAA*, VERIFY (May 19, 2022), https://www.verifythis.com/article/news/verify/health-verify/

Among the top twenty downloaded period tracking apps, there is one app that may be protected under HIPAA in certain circumstances.[59] The Ovia Health app is deemed connected to a covered entity if an individual receives the app as a benefit from their health plan or health care provider.[60]

Some period tracking apps claim to be HIPAA compliant; however, such language is misleading. Claiming HIPAA compliance is meaningless if the app is not associated with a HIPAA-covered entity.[61] In fact, such claims of HIPAA compliance could be construed as misleading to consumers by the FTC.

Federal legislative action to expand HIPAA could close this gap in protecting sensitive health information collected by mobile health apps. Alexis Guadarrama has proposed replacing the "covered"/"non-covered" paradigm with one that focuses on the type of data collected rather than the status of the collector.[62] Without replacing the covered/non-covered dichotomy, expansions of HIPAA regarding reproductive health care privacy—including the current proposed rulemaking from the Office for Civil Rights at the U.S. Department of Health to modify HIPAA to strengthen reproductive healthcare privacy—will not extend to reproductive health care information collected on period tracking or other mobile health apps.[63]

---

period-tracking-apps-hipaa-privacy-rules-law-fact-check/536-bf44e08c-cc5f-4ee8-997a-c15e00 60081a.

59. *Id.*

60. *Id.*; *see also* Ovia Health Privacy Policy, https://www.oviahealth.com/privacy-policy/.

61. Jones, *supra* note 58, see *also* Guadarrama, *supra* note 9 at 1005.

62. Guadarrama s*upra* note 9 at 1020.

63. Guadarrama, *supra* note 9 at 1020; *see* HIPAA Privacy Rule Notice of Proposed Rulemaking to Support Reproductive Health Care Privacy Fact Sheet, U.S. Department of Health and Human Services U.S. Department of Health and Human Services (Apr. 25, 2023), https://www.hhs.gov/hipaa/for-professionals/regulatory-initiatives/hipaa-reproductive-health-fact-sheet/index.html. (The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) issued a notice of proposed rulemaking to modify HIPAA to strengthen reproductive health care privacy. The proposed rule is being drafted pursuant to President Biden's executive order issued weeks after *Dobbs v. Jackson Women's Health Organization* to better protect sensitive information related to reproductive health care and bolster patient-provider confidentiality. Under the proposed rule, protection of reproductive health care information would apply in relevant criminal, civil, or administrative investigations or proceedings in connection with (1) reproductive health care that is sought, obtained, provided, or facilitated in a state where the health care is lawful and outside of a state where the investigation or proceeding is authorized; (2) reproductive health care that is protected, required, or expressly authorized by federal law, regardless of the state in which such health care is provided; and (3) reproductive health care that

B. Fourth Amendment Limitations

Fourth Amendment protections from warrantless searches are limited to searches of places and items in which people have a reasonable expectation of privacy.[64] With regard to sensitive health data, Fourth Amendment protections have been limited.[65] Law enforcement officers generally do not need probable cause and a warrant to access companies' databases of health information.[66] Typically, only a subpoena is needed to access these databases.[67]

While the Supreme Court has recognized that technological advancements have made personal information exponentially more accessible to law enforcement over the last decade, health information from period tracking apps is unlikely to be considered reasonably private to consumers due to the Supreme Court's narrow holding in *Carpenter v. United States*.[68]

In response to technological advances, the Supreme Court's decision in *Carpenter v. United States* changed how the Fourth Amendment is applied to new and disruptive technologies.[69] The Court reasoned that to determine whether technology enables unreasonable searches, the focus should be on the technology itself, its level of advancement, what information it can reveal about our lives, and how it collects and stores information.[70] Essentially, if a technology enables police surveillance that is "too permeating," it will likely be considered an unreasonable search under *Carpenter* protection.[71]

The Court focused on whether technology changed expectations of what police can do.[72] If seized data goes beyond information that is

is provided in the state where the investigation or proceeding is authorized and is permitted by the law of the state in which such health care is provided.).

64. Aparna Bhattacharya, *The Impact of* Carpenter v. United States *on Digital Age Technologies*, 29 S. CAL. INTERDISC. L.J. 489, 489-514 (2019).

65. Ryan Knox, *Fourth Amendment Protections of Health Information After* Carpenter v. United States*: The Devil's in the Database*, 45 AM. J. L. & MED., 331, 331-355, (2019).

66. *Id.* at 333.

67. *Id.*

68. *Id.* at 333-34.

69. *Id.* at 344.

70. *Id.*

71. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018); s*ee further*, Stored Communications Act, 18 U.S.C. 2703(d)(2019) (the government can obtain an individual's records without a warrant or probable cause if it can show that the evidence is reasonably related to a criminal investigation).

72. *Id.*

reasonably required to pursue a criminal investigation, then the data will have a reasonable expectation of privacy associated with it.[73]

While the Court narrowly limited its holding in *Carpenter* to historical cell-site location information, the Court did express in dicta concerns about advanced technology allowing access to private health information.[74] However, the Supreme Court has not to date had the opportunity to consider the *Carpenter* protection with regard to health information.[75]

While the Carpenter decision altered how the Fourth Amendment applies to new technologies, *Carpenter* protection will likely not extend to sensitive health data. To obtain Fourth Amendment protection under *Carpenter*:

> (1) the collection of information must have been made widely possible by surveillance methods of the digital age; (2) the records must not be the product of a user's meaningful voluntary choice; (3) the records must be of a type that tends to reveal an intimate portrait of a person's life beyond the legitimate interest of criminal investigation . . . such as our personal associations, religious beliefs, sexual preferences, and political views.[76]

Looking at the first prong, to receive *Carpenter* protection, the technology in question must be novel or highly transformative.[77] Early surveillance tools, despite their potentially revealing nature, do not qualify. It is challenging to determine which technologies should be included or excluded when significant advancements have occurred in the technology industry. Regarding period tracking apps, while the process of tracking a menstrual cycle is not new, the extent of data collection and analysis possible with these apps is a product of digital age-methods rather than the surveillance methods of an earlier time. After all, users consent to the app's storage, retention, and disclosure of their health information by agreeing to the terms and conditions of period tracking

73. *Id.* at 2217 ("provides an intimate window into a person's life").

74. *Id.* at 2218 (Although *Carpenter* did not concern health information, Chief Justice Roberts and Justice Gorsuch contemplated the decision's impact on health information privacy, indicating that doctors offices raise special privacy concerns).

75. *See further*, Smith v. Maryland, 99 S.Ct. 2577 (1979) and United States v. Miller, 96 S.Ct 1619 (1976) (A person does not have a legitimate expectation of privacy in information he voluntarily turns over to third parties. Therefore, the government can obtain information directly from third parties without having probable cause or obtaining a warrant. SCOTUS declined to extend *Smith* and *Miller* to *Carpenter* because *Smith* and *Miller* were decided before seismic shifts in digital technology.).

76. Bhattacharya, *supra* note 64 at 494.

77. *Id.* at 494-95.

apps. The sensitive health data collected by health and period tracking apps does not meet the second prong when these apps provide reasonable notice to users through their privacy policies and terms of use.

Regarding the third prong, information collected by period tracking apps certainly reveals an "intimate portrait of a person's life." These apps gather myriad sensitive health information, such as when a user is or is not menstruating, is or is not pregnant, or is on or off birth control. They also collect intimate user information related to symptoms of premenstrual and menstrual syndrome symptoms, including mood, sex drive, acne, cramps, cravings, and flow.

While some of the sensitive health information collected by period tracking apps would likely be beyond the "legitimate interest of criminal investigation," certain data on pregnancy status would likely be considered of legitimate interest in the criminal investigation of an illegal abortion.

Carpenter protection will likely not extend to period tracking apps' collection of pregnancy status due to the analysis of privacy rights in relation to abortion in the *Dobbs* decision. In *Dobbs*, the Supreme Court held that abortion is distinct from other rights purportedly rooted in privacy and autonomy because of the moral questions related to fetal life.[78] Therefore, if abortion is distinct from privacy rights, then subpoenas for health data from period tracking apps will likely not be protected by the Fourth Amendment, at least where criminal investigations regarding illegal abortions are concerned.

IV. PROPOSED FEDERAL DATA PRIVACY LEGISLATION

There are several proposed pieces of federal data privacy legislation that have been introduced since the *Dobbs* decision in 2022. While none of them has yet passed through the House or Senate, they provide useful insights into the frameworks Congress is considering for potential future federal data privacy laws. This section analyzes three recent proposed federal data privacy laws, examining how they would apply to mobile health and period tracking apps.

A. Health and Location Data Protection Act (2022)

The Health and Location Data Protection Act aims to ban data brokers from selling Americans' health and location data.[79] The bill,

78. Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228, 2258 (2022).

79. The term "data broker" means a person that collects, buys, licenses, or infers data about individuals and then sells, licenses, or trades that data. Steve Alder, Bill Seeks to Bad Data

which was sponsored by senators Warren, Wyden, Murray, Whitehouse, and Sanders in July 2022, was drafted in response to the largely unregulated collection and sale of sensitive health information and location data by data brokers.[80] "If passed, the Health and Location Data Protection Act will ban brokers from selling or transferring both health and location data."[81]

The bill empowers the FTC, state attorneys general, and injured persons to sue data brokers to enforce the provisions of the law.[82] A violation of the act would be treated as a violation of a rule defining an unfair or deceptive act or practice under section 18 of the Federal Trade Commission Act.

The bill does not cover actions that are HIPAA compliant, so the regulation of health information associated with covered entities remains unchanged.[83] The Health and Location Data Protection Act would primarily address the protection of sensitive health information gathered by mobile health apps. Under this bill, period tracking apps would be prohibited from selling, reselling, licensing, trading, transferring, or sharing user data with third parties. The bill has been "read twice and referred to the Committee on Commerce, Science, and Transportation."[84]

B. American Data Privacy and Protection Act (2021-2022)

The American Data Privacy and Protection Act (ADPPA) is Congress's latest attempt to establish a comprehensive federal data privacy law.[85] The bill was released in June 2022 with bipartisan support from both the Senate and House Commerce committees.[86] The ADPPA would apply broadly to entities that collect, process, or transfer covered data.[87] The bill defines "covered data" as "information that identifies or is linked or reasonably linkable, . . . to an individual or a device . . .

Brokers from Selling Health and Location Data, THE HIPAA J. (June 17, 2022), https://www.hipaajournal.com/bill-seeks-to-ban-data-brokers-from-selling-health-and-location-data/ (bill introduced by Senator Elizabeth Warren and cosponsored by senators Ron Wyden, Patty Murray, Sheldon Whitehouse, and Bernie Sanders).

80. *Id.*

81. *Id.*

82. Health and Data Protection Act of 2022, S.4408, 117th Cong. §3(a) (2022).

83. *Id.* §2(b)(1).

84. Health and Data Protection Act of 2022 Actions, S.4408, 117th Cong. (2022), https://www.congress.gov/bill/117th congress/senate-bill/4408/all-actions?s=1&r=60.

85. American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

86. *Id.* (sponsored by House Representatives Pallone, Rodgers, Schakowksy, and Bilirakis).

87. *Id.* §§2(26),(29),(35); 103(a)(1),(a)(4).

reasonably linkable to an individual," including derived data and unique identifiers.[88] Significantly, the bill also considers health information to be "sensitive covered data."[89]

ADPPA was drafted to provide consumers with data privacy rights and to create oversight and enforcement mechanisms.[90] The act states that the transfer of sensitive data to third parties is impermissible without the "express consent of the individual."[91] This loyalty duty would change how period and health tracking apps notify consumers about the transfer of sensitive data to third parties.[92] However, the proposed bill also includes compliance with legal obligations or investigations in its list of permissive purposes for collecting, processing, or transferring personal data.[93] Therefore, transferring sensitive reproductive health information to authorities in connection with an investigation or legal proceeding would likely be permissible under this proposed legislation. The proposed legislation was referred to the House Committee on Energy and Commerce and the Subcommittee on Consumer Protection and Commerce, and it was introduced to the House of Representatives in June 2022.

C. My Body, My Data Act—H.R. 8111, 117th Cong. (2023)

The My Body, My Data Act is a bill designed to protect the privacy of personal reproductive and/or sexual health information. The bill was sponsored by House Representative Sara Jacobs of California and has 112 Democratic cosponsors. The proposed legislation, if passed, would limit the personal reproductive and sexual health data that can be collected, retained, used, or disclosed to only what is needed to deliver a product or service; require regulated entities to develop and share a privacy policy outlining how they collect, retain, use, and disclose personal reproductive health information; and provide the right of an individual to access and delete their personal data.[94]

88. Derived data is new data created by combining and processing existing raw data. A unique identifier (UID) is a numeric or alphanumeric string that is associated with a single entity within a given system. UIDs make it possible to address that entity, so that it can be accessed and interacted with. *Id.* §2(8).

89. American Data Privacy and Protection Act, *supra* note 85 §102(3).

90. The proposed legislation would also create within the FTC a Bureau of Privacy, which would assist the FTC in enforcing the act's proposed data privacy regulations. *Id.* §104(a).

91. American Data Privacy and Protection Act, *supra* note 85 §102(3)(A).

92. *Id.* §102(3).

93. *Id.* §102(3)(b).

94. *See generally* My Body, My Data Act of 2023, H.R. 3420, 118th Cong. (2023).

The bill directs the FTC to enforce the law and develop rules for implementing the statute, creating a private right of action that allows individuals to hold regulated entities accountable for violations.[95] Additionally, the bill includes a non-preemption clause that permits states to offer further protection for reproductive sexual health privacy.[96]

While the My Body, My Data act prohibits mobile health apps from collecting, retaining, using, or disclosing personal reproductive or sexual health information, the prohibition does not apply to collation, retention, use, or disclosure that is "strictly necessary to provide a product or service that the individual" requested from the app.[97] It is unclear what user data would be considered "strictly necessary" for mobile health apps to collect, retain, use, disclose with regard to the services requested by users. Furthermore, the My Body, My Data act does not prohibit the transfer or sale of user health information to third parties if deemed "strictly necessary." The proposed legislation only requires that the mobile health apps disclose to consumers exactly which third parties their data was shared with and why.[98]

Additionally, the My Body, My Data Act is a narrow piece of legislation, addressing only the protection of reproductive or sexual health information.[99] The bill does not extend to other types of sensitive health information collected by period tracking apps or other mobile health apps.[100]

V. PROTECTING REPRODUCTIVE HEALTH DATA IN LOUISIANA

A. Abortion Access in Louisiana

LA R.S. 14:87.7 outlines the parameters for unlawful abortion in Louisiana and the penalties for those who commit such acts.[101] This statute applies only to physicians or other persons who perform the abortion, not to the pregnant female on whom an unlawful abortion is committed or performed. Exceptions to R.S. 14:87.1 are detailed in § 1061.23 Emergency, which compels the immediate performance of an

95. *Id.* §6(a).
96. *Id.* §9(b).
97. *Id.* §2(a).
98. *Id.* §§4-5.
99. *See generally* H.R. 3420.
100. The bill does not alter existing HIPAA protections for sensitive health information collected by covered entities or businesses associated with covered entities. *Id.* §7(b).
101. *See further* LA. REV. STAT. tit. 14 §87.1; *see also* LA. REV. STAT. tit. 14 §87.7

abortion when continuing the pregnancy poses an immediate threat and grave risk to the life or serious health of the pregnant person.[102]

B. Louisiana Data Privacy Laws

The right to privacy is protected by Article 1(5) of the *L*ouisiana Constitution of 1974. Louisiana has only one privacy law specifically related to data privacy and security. The Louisiana Database Security Breach Notification Law requires persons who conduct business in the state and who "own or license computerized data that includes personal information" to notify state residents of breaches of their personal information.[103]

Louisiana's confidentiality of medical information statute works alongside HIPAA to protect health information from disclosure only when that information pertains to diagnosis, treatment, or health and is obtained by a health care provider or organization.[104] Neither HIPAA nor the Louisiana confidentiality of medical information statute offers a framework for safeguarding health data collected by mobile health apps.[105]

C. Recommendations—Legislative Reform

1. Looking Towards California, Virginia, and Colorado as Examples

a. California Consumer Privacy Act

The California Consumer Privacy Act (CCPA) was the first comprehensive consumer privacy legislation in the United States.[106] Recently amended by the California Privacy Rights Act (CPRA), this California provision sets the standard for how many businesses approach data privacy and security.[107] The CCPA encompasses a range of consumer privacy rights and business obligations regarding the collection and sale of personal information.[108] The revised provision established the

102. *See also* LA. CONST. art. I §20.1 ("To protect human life, nothing in this constitution shall be constructed to secure or protect a right to abortion or require the funding of abortion.").

103. The law also requires these businesses to report data breaches to the Louisiana attorney general; failure to do so may result in a fine of up to $5,000 per day. LA. REV. STAT. tit. 51 §3074.

104. *See* LA. REV. STAT. tit. 22 §265.

105. *Id.*

106. *California Consumer Privacy Act* (CCPA), STATE OF CALIFORNIA DEPARTMENT OF JUSTICE (Mar. 13, 2024), https://oag.ca.gov/privacy/ccpa.

107. *Id.*

108. *See generally* California Privacy Rights Act (CPRA) of 2020, CAL. CIV. §1798.

California Privacy Protection Agency and became effective in January 2023. Under the CCPA, consumers have eight specified rights:

> 1. The right to know (request disclosure of) personal information collected by the business about the consumer, from whom it was collected, why it was collected, and, if sold, to whom;
>
> 2. The right to delete personal information collected from the consumer;
>
> 3. The right to opt out of the sale of personal information (if applicable);
>
> 4. The right to opt in to the sale of personal information of consumers under the age of sixteen (if applicable);
>
> 5. The right to nondiscriminatory treatment for exercising any rights;
>
> 6. The right to initiate a private cause of action for data breaches;
>
> 7. The right to correct inaccurate personal information;
>
> 8. The right to limit the use and disclosure of sensitive personal information for purposes required to provide users with services requested.[109]

Under the CCPA, sensitive personal information includes the processing of biometric information for the purpose of uniquely identifying a consumer, personal information collected and analyzed concerning a consumer's health, and personal information collected and analyzed concerning a consumer's sex life or sexual orientation.[110]

b. Virginia Consumer Data Protection Act

The Virginia Consumer Data Protection Act (VCDPA), which went into effect in January 2023, provides Virginia residents with rights regarding personal data collected by businesses. The VCDPA allows for consumers to request that the controller of their personal data: (1) confirm if the controller is actually processing their personal data, (2) correct inaccuracies in the consumer's personal data collected by the controller, (3) delete personal data provided by or obtained about the consumer,(4) obtain copies of the personal data collected by the controller, and (5) opt out of the processing of personal data for the purposes of targeted advertising, the sale of personal data, or further profiling.[111]

109. *See id.* §§1-8.

110. *See id.* §14.

111. *See generally* Consumer Data Protection Act (VCDPA), VA. CODE ANN. §59.1-577 (2023).

The VCDPA also provides for the protection of sensitive data subject to additional requirements. Controllers cannot process sensitive data concerning a consumer without obtaining the consumer's consent.[112] The VCDPA considers the following to be sensitive data: (1) a person's racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; (2) the processing of genetic or biometric data for the purposes of uniquely identifying that person; (3) the personal data collected from a known child, which is defined as someone younger than thirteen years old; and (4) precise geolocation data.[113]

c. Colorado Privacy Act

Effective July 2023, the Colorado Privacy Act (CPA) grants Colorado consumers rights regarding their personal data, including the right to access, delete, and correct their personal data, as well as the right to opt out of the sale of their personal data or its use for targeted advertising or profiling.[114] The CPA also requires certain covered entities to safeguard consumer personal data by providing consumers with meaningful disclosures about the use of their data, conducting data protection assessments, and obtaining consent before processing sensitive personal data.[115] Sensitive data under the CPA includes information about an individual's sexual orientation and health diagnoses.[116] The CPA specifies that controllers shall not process sensitive data without first obtaining consent from the consumer.[117]

2. Proposal for Louisiana Consumer Privacy Act

Louisiana currently has no data privacy laws regulating the collection and use of consumer data. Establishing a regulatory framework would implement measures to better protect the personal and sensitive health information of Louisiana residents.

Based on both the proposed federal data privacy legislation and existing state data privacy laws, a data privacy law for Louisiana should provide consumers with: (1) the right to know what personal information a business collects and how that information is used, stored, and disclosed

112. *Id.* § 59.1-578.

113. *Id.* §59.1-575.

114. Colorado Privacy Act, COLO. REV. STAT. ANN. 6-1-1302 (2023).

115. *Id.*

116. *Id.* §6-1-1303.

117. Or in the case of a known child, consent from the child's parent or lawful guardian is needed. *Id.* §6-1-1308.

by the collector; (2) the right to review, correct, and delete personal information collected; and (3) the right to opt out of sharing personal information with third parties. A Louisiana data privacy law should also prohibit collectors from processing sensitive health information without the express consent of consumers.

As with the proposed federal and existing state data privacy laws, the creation of a data privacy law in Louisiana would not necessarily limit the ability of law enforcement to acquire sensitive health information in connection with a criminal investigation. Nevertheless, measures to increase transparency regarding the information gathered, stored, and shared by data collectors would enable consumers to make more informed decisions about how they want to interact with data collection businesses such as mobile health apps. Additionally, the ability to opt out of third-party sharing would reduce the vulnerability of personal and sensitive health information from breaches by bad actors, as this provision would allow users to limit data storage to local, personal devices.

VI. CONCLUSION

While period tracking apps are marketed as helping women to monitor and manage their reproductive health, the lack of regulation regarding how these apps handle users' sensitive reproductive health information raises privacy concerns.

With the Supreme Court's *Dobbs* decision overturning *Roe v. Wade*, privacy concerns intensified regarding who has access to individuals' reproductive health information and for what purposes can they use that information. With abortion criminalized in some states, sensitive health information collected by period tracking apps can now be shared not only with third-party holders and advertisers, but also with law enforcement in cooperation with criminal investigations of illegal abortions.

Since the *Dobbs* decision was announced, federal data privacy legislation has been proposed, and states have enacted laws in response to concerns about the privacy of personal and sensitive health information. Such data privacy laws are essential for protecting personal and sensitive health information, because the information collected by mobile health apps is not protected by HIPAA and likely not covered by Fourth Amendment protections.

Louisiana, which has only one data privacy law related to breaches, could benefit from legislation regulating the collection of residents' personal and sensitive health information. Such legislation would likely not prevent law enforcement or prosecutors from obtaining personal or

sensitive health information in relation to a criminal investigation or legal proceeding; however, data privacy legislation would promote transparency and choice for consumers in limiting third-party sharing. Regulation of data collection would allow Louisiana residents to make more informed decisions on how the want to interact with data collection businesses such as mobile health apps. The ability to opt out of or limit third-party sharing would also decrease the vulnerability of Louisiana residents' personal and sensitive health information from breach. A Louisiana data privacy law that provides consumers with (1) the right to know what personal information a business collects and how that information is used, stored, and disclosed by the collector; (2) the right to review, correct, and delete personal information collected; and (3) the right to opt-out of sharing personal information with third-parties and that also prohibits collectors from processing sensitive health information without consumers' consent, would promote transparency and data security for residents who interact with period tracking apps, mobile health apps, and other data collection businesses.