Santa Clara University School of Law

Santa Clara Law Review

Volume 64 | Number 1 Article 6

2024

LIES, DAMN LIES, AND PRIVACY PROMISES

Rash, Andy

Fowler, Leah R.

LIES, DAMN LIES, AND PRIVACY PROMISES

Andy Rash* and Leah R. Fowler**

*Health apps and other consumer technologies collect massive amounts of sensitive data, including but not limited to information about users' reproductive lives. As a result, consumer choices—especially for menstruation tracking applications—are at least partly driven by privacy promises in advertising and privacy policies. But there is a problem: whether these promises are grounded in reality can often only be revealed by complex analyses outside the capabilities of the majority of consumers and, even then, may be unknowable in any definitive sense. This essay explores this problem in the context of menstruation tracking applications and post-*Dobbs *legal developments that implicate reproductive data. In it, we question the adequacy of existing laws and regulations and the limitations of even the most robust proposed legislation and underscore that if we cannot solve the problem of privacy lies, any hard-fought reforms will be hollow.*

* J.D. Candidate 2024, University of Houston Law Center; B.S., Computer Science, Southern Methodist University

* * Research Assistant Professor, University of Houston Law Center, and Research Director, Health Law & Policy Institute

We would like to thank the organizers and participants of the Santa Clara Law Review 2023 Annual Symposium on Navigating the Post-*Dobbs* Landscape and the student editors of the Santa Clara Law Review. This research was made possible by an internal grant award from the University of Houston. All errors are our own.

TABLE OF CONTENTS

I. INTRODUCTION

The same day the Supreme Court handed down its opinion in *Dobbs v. Jackson Women's Health Organization*,[1] the astrology-focused period tracking app, *Stardust*,[2] announced that it had implemented end-to-end encryption for its users' data.[3] In the two days that followed, it experienced hundreds of thousands of downloads, accounting for eighty-two percent of its lifetime installs and skyrocketing the app to number one in the Apple App Store rankings.[4] This mass migration to *Stardust* suggests consumers were not heeding the onslaught of news and social media headlines imploring them to delete their period-tracking apps.[5] Instead, they were opting for apps advertising better privacy protections. But there was one big problem: *Stardust* never truly offered end-to-end encryption.[6]

1. Dobbs v. Jackson Womens Health Organization, 142 S. Ct. 2228 (2022).

2. Stardust Period Tracker App, Stardust App LLC, https://apps.apple.com/us/app/stardust-period-tracker/id1495829322.

3. Sarah Perez & Zack Whittaker, *Period Tracker Stardust Surges Following Roe Reversal, But Its Privacy Claims Aren't Airtight,* TechCrunch (June 27, 2022) https://techcrunch.com/2022/06/27/stardust-period-tracker-phone-number/.

4. *Id.*

5. *See, e.g.,* Nicole Westman and Victoria Song, *How to delete your period tracking app data,* The Verge (June 30, 2022) https://www.theverge.com/2022/6/30/23190142/delete-period-tracking-app-roe-v-wade-how-to (observing that "Warnings to delete cycle tracking apps flooded social media in the wake of the United States Supreme Court's decision to overturn *Roe v. Wade* and end federal abortion protections.").

6. *Id; see, e.g.*, Taggart (@MTTaggart), TWITTER (July 1, 2022, 11:17 AM), https://twitter.com/mttaggart/status/1542935504353497088?s=11&t=aUiWNRzd1EwNWLdQEB2aDA (providing a step-by-step examination of the technical aspects of the app's alleged encryption and ultimately concluding the data is "lightly anonymized" and would be unlikely to withstand a subpoena or warrant).

Though *Stardust*'s founder later divulged the use of encryption at some stages of their data pipeline,[7] a subsequent third-party investigation revealed that the app sent users' individual encryption keys to *Stardust*'s servers, meaning that the company (or whoever later came into possession of those keys) could decrypt users' data.[8] The company later quietly updated its privacy policy to remove mentions of end-to-end encryption.[9]

Though the points of dispute may seem highly technical, and perhaps even like splitting hairs, they are emblematic of a larger problem of advertising privacy protections that misrepresent a company's data-sharing practices. Make no mistake, *Stardust* is far from alone and is certainly not the worst offender. Within a health app context, researchers have described the phenomenon in depression and smoking cessation apps,[10] diabetes apps,[11] and others. And the problem extends far beyond health apps. Some of the biggest players in technology—like Google[12] and Meta[13]—make privacy promises they cannot seem to keep. Even Apple, often holding itself out as a leader in privacy,[14] has more recently come under scrutiny for overstating its privacy protections.[15] But menstrual trackers like *Stardust* and the intimate data they contain

7. Perez & Whittaker, *supra* note 3.

8. *Id*.

9. *Id*.

10. Kit Huckvale, John Torous, & Mark E. Larsen, *Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation*, JAMA NETW OPEN. https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2730782.

11. Sarah R. Blenner et al., *Privacy Policies of Android Diabetes Apps and Sharing of Health Information*, 315(10) JAMA 1051 (2016).

12. Geoffrey A. Fowler, *Google promised to delete sensitive data. It logged my abortion clinic visit.*, WASHINGTON POST (May 9, 2023 11:23 a.m. EDT), https://www.washingtonpost.com/technology/2023/05/09/google-privacy-abortion-data.

13. *FTC Proposes Blanket Prohibition Preventing Facebook from Monetizing Youth Data,* Federal Trade Commission, (May 3, 2023) https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-proposes-blanket-prohibition-preventing-facebook-monetizing-youth-data.

14. *See, e.g.*, Russell Brandom, *Apple wants to be the only tech company you trust*, THE VERGE (Mar. 26, 2021 8:31 AM CDT), https://www.theverge.com/2019/3/26/18282158/apple-services-privacy-credit-card-tv-data-sharing.

15. Thomas Germain, *Apple Is Tracking You Even When Its Own Privacy Settings Say It's Not, New Research Says*, GIZMODO (Nov. 8, 2022), https://gizmodo.com/apple-iphone-analytics-tracking-even-when-off-app-store-1849757558.

shock the conscience in a way that other technologies do not,[16] and growing restrictions on reproductive rights make clear that the risks are real and extend far beyond unwanted targeted advertisements.[17]

It is not brave or controversial to assert that consumers should be able to trust a product's claims about the privacy protections it offers. Indeed, lying about or misrepresenting privacy protections is already illegal, even in the United States[18], where privacy laws, though growing in number, are piecemeal and often limited. But the practice is widespread, fueled by the incredible monetary value of consumer data generally[19] and reproductive data specifically.[20] The Federal Trade Commission (FTC), perhaps the agency best situated to curb this behavior, knows that deceptive third-party data sharing is pervasive.[21] But the FTC's ability to act and its bold

16. Other esteemed scholars have long noted the unique issues that arise in the context of intimate data and sexual privacy. *See, e.g.*, Karen E. C. Levy, *Intimate Surveillance,* 51 IDAHO L. REV. 679, 686-87 (2015); *see also* Danielle Keats Citron, *A New Compact for Sexual Privacy*, 62 WM. & MARY L. REV. 1763, 1771-72 (2021) [hereinafter Danielle Keats Citron, *New Compact*]; Danielle Keats Citron, *Sexual Privacy*, 128 YALE L. J. 1870, 1944-54 (2019); *See also* Michele Estrin Gilman, *Periods for Profit and the Rise of Menstrual Surveillance,* 41 COLUM. J. GENDER & L. 100 (2021).

17. *See generally* Danielle Keats Citron, *Intimate Privacy in a Post-*Roe *World,* FL. L. REV (forthcoming).

18. For example, in May 2023, the Federal Trade Commission started settlement proceedings with app developer Easy Healthcare Corporation, alleging among other things that statements in its privacy policy were false or deceptive relative to its actual business practices. *See* Complaint for Permanent Injunction, Civ. Penalty Judgment, and Other Relief, United States v. Easy Healthcare Corp., No. 1:23-cv-03107 (N.D. Ill. May 17, 2023).

19. The data broker market alone is expected to reach over $365 billion by 2029. *Data Broker Market: Global Industry Forecast (2023-2029) by Data Category, Data Type, Pricing Model, End Use Sector, and Region*, MAXIMIZE MKT. RSCH., https://www.maximizemarketresearch.com/market-report/global-data-broker-market/55670.

20. *No Body's Business But Mine: How Menstruation Apps Are Sharing Your Data*, PRIV. INT'L, https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruations-apps-are-sharing-your-data (last updated Oct. 7, 2020); *see also* Matt Petronzio, *How One Woman Hid Her Pregnancy From Big Data*, MASHABLE (Apr. 26, 2014), https://mashable.com/archive/big-data-pregnancy ("According to Vertesi, the average person's marketing data is worth 10 cents; a pregnant woman's data skyrockets to $1.50.").

21. The FTC is the agency arguably best equipped to address these practices on a nationwide level. *See, e.g., Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking*, OFF. OF TECH, FED. TRADE COMM'N (Mar. 16, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking.

statements about holding companies to their promises[22] may be little more than an empty threat in light of the agency's resource limitations and the vast and ever-growing number of consumer technologies available for download.[23] As a result, companies may feel empowered to continue making promises they cannot—or perhaps never had the intention to—keep.

Whether period and fertility tracking apps or consumer health technologies more broadly advertise data privacy protections and whether they actually provide those protections in any meaningful way are many times—though not always[24]—empirical questions. By highlighting the unique challenges of period trackers within the larger problem of privacy lies and misrepresentations, this paper illustrates what happens when an app developer's empty promises meet enforcement's empty threats. Caught in the middle are vulnerable people who would need to have an unreasonably

22. *Developer of Popular Women's Fertility-Tracking App Settles FTC Allegations that It Misled 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 (quoting Andrew Smith, Director of the FTC's Bureau of Consumer Protection, as saying "Apps that collect, use, and share sensitive health information can provide valuable services, but consumers need to be able to trust these apps […] We are looking closely at whether developers of health apps are keeping their promises and handling sensitive health information responsibly.").

23. The FTC operates with fairly limited resources, so it prioritizes only the most significant and impactful cases. U.S. FED. TRADE COMM'N, FTC REPORT TO CONGRESS ON PRIVACY AND SECURITY 3–6 (2021), https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf (describing the FTC's priorities in privacy and security and noting that they "focus most of [their] limited resources on the most egregious practices and cases against major players in the marketplace in order to have a broad impact"); *see also FTC Appropriation and Full-Time Equivalent (FTE) History*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/bureaus-offices/office-executive-director/financial-management-office/ftc-appropriation (last visited Apr. 14, 2023) (showing how, starting in 1979 and continuing throughout the 1980s, the FTC's reported Full-Time Equivalent (FTE)—essentially a measure of the agency's available bandwidth to do its job—dropped precipitously from its high-water mark of 1,746, and it has only partially recovered, stabilizing around 1,100 between 2008 and 2022).

24. In some cases, the answer to what happens to data after it leaves a device or where it goes is unknowable, even by the companies who created the data infrastructure. *See, e.g.,* Lorenzo Franceschi-Bicchierai, *Facebook Doesn't Know What It Does With Your Data, Or Where It Goes: Leaked Document*, VICE: MOTHERBOARD (Apr. 26, 2022, 8:02am), https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes.

high level of technological competence to appreciate the risks fully. That is, if they can ever truly know the risks at all.[25]

This paper proceeds in three parts. Part II introduces one method of assessing privacy promises and research relevant to understanding surreptitious third-party data sharing. To do so, we give an overview of some important technical concepts and then briefly describe a snapshot of the scientific literature demonstrating our concern in areas outside of period and fertility tracking apps. In Part III, we consider the increased importance these issues take on in the post-*Dobbs* legal landscape. In it, we turn to period and fertility trackers, interrogate what the research suggests about deceptive data sharing in this product category, and assess the implications of those data in light of retrenchments in reproductive rights. Part IV then considers how existing legal mechanisms handle these challenges at the state and federal level, underscoring some areas where they are successful and others where they fall short. This paper uses femtech as a case study to identify a significant disconnect between the legal fictions governing consumer technologies and consent and the darker reality. But many of the behaviors we identify in this paper are *already* illegal, calling into question whether current and proposed approaches are truly sufficient. We conclude by emphasizing the importance of researchers and journalists in augmenting state and federal efforts as a stopgap measure and encourage readers to consider this problem beyond *Dobbs*.

II. PRIVACY'S [SOMETIMES] EMPTY PROMISES

Despite what some corners of the technology industry and their interest groups might have you believe,[26] consumers do value privacy.[27] Many of these companies spend resources

25. Kit Huckvale, et al. *Unaddressed Privacy Risks in Accredited Health and Wellness Apps: A Cross-Sectional Systematic Assessment,* BMC MED. 13:214 (2015) (observing that "because users cannot see into the inner workings of apps, or the services they connect to, confidence that personal information is handled appropriately relies mostly on trust").

26. *See, e.g.*, Neil Sahota, *Privacy Is Dead and Most People Really Don't Care*, FORBES (Oct. 14, 2020 08:00am EDT), https://www.forbes.com/sites/neilsahota/2020/10/14/privacy-is-dead-and-most-people-really-dont-care/?sh=575be6617b73 (arguing that "[consumers] don't truly value privacy as much as we like to believe we do").

27. One case study appeared with Apple's release of iOS 14.5 in April 2021, an update which introduced a feature that required users to opt in before apps could track their data across apps or websites. *iOS 14.5 delivers Unlock iPhone*

advertising privacy features to consumers, suggesting they likely already know this.[28] But the type and quantity of data that come from a more relaxed approach to privacy are likewise immensely valuable to developers and advertisers.[29] This creates tension between consumer and developer interests.[30] Perhaps predictably, the result is partial truths, clever omissions, and shady business practices in the pursuit of data collection that are well-documented in the literature and agency enforcement actions.[31] This Part introduces the problem of third-party data sharing that contradicts consumer-facing messaging and privacy policy terms. Here, we explain what we mean when discussing third-party data sharing and how—and to what extent—we can assess it. We then turn to a few examples of scientific studies documenting this type of deceptive behavior.

A. Surreptitious Data Sharing

We could highlight many aspects of privacy and security, including vulnerabilities that lead to illicit access by malicious users,[32] voluntary data sharing through synced companion

---

with Apple Watch, more diverse Siri voice options, and new privacy controls, APPLE (Apr. 26, 2021), https://www.apple.com/newsroom/2021/04/ios-14-5-offers-unlock-iphone-with-apple-watch-diverse-siri-voices-and-more. In the weeks that followed, app analytics company Flurry found that only 6% of users chose to allow tracking. *iOS 14.5 Opt-in Rate – Daily Updates Since Launch*, Flurry (May 25, 2021), https://www.flurry.com/blog/ios-14-5-opt-in-rate-att-restricted-app-tracking-transparency-worldwide-us-daily-latest-update. In other words, when given the choice of whether to be tracked, 94% of users opted out.

28. For a series of articles exploring and justifying the idea that companies market what consumers value, *see* Jim Hawkins & Renee Knake, *The Behavioral Economics of Lawyer Advertising: An Empirical Assessment*, 2019 U. ILL. L. REV. 1005 (2019); *see also* Jim Hawkins, *Exploiting Advertising*, 80 LAW & CONTEMP. PROBS. 43 (2017); *see also* Jim Hawkins, *Using Advertisements to Diagnose Behavioral Market Failure in the Payday Lending Market*, 51 WAKE FOREST L. REV. 57 (2016).

29. Maximize Market Research, *supra* note 19.

30. *See, e.g.,* Nils Wernerfelt, Anna Tuchman, Bradley Shapiro & Robert Moakler, *Estimating the Value of Offsite Data to Advertisers on Meta* 4 (U. Chi., Becker Friedman Inst. for Econ., Working Paper No. 114, 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4198438 (estimating that advertisers need to spend roughly 37% more to gain new customers when privacy regulations prohibit access to detailed consumer data).

31. *See* discussion *infra* Parts III.B., IV.A

32. *See, e.g.*, Jerry Beilinson, *Glow Pregnancy App Exposed Women to Privacy Threats, Consumer Reports Finds*, CONSUMER REPORTS (Sept. 17, 2020), https://www.consumerreports.org/electronics-computers/mobile-security-software/glow-pregnancy-app-exposed-women-to-privacy-threats-a1100919965/.

accounts,[33] or matters involving warrants and subpoenas,[34] among others.[35] However, in this paper, we focus exclusively on third-party data sharing, though we acknowledge that some of these issues can and do overlap.[36] In particular, this Part considers circumstances in which a company represents that it will treat data one way and then does something different. Here, we introduce what third-party data sharing is, how it is used, and a common approach used in research to assess third-party data-sharing practices. We then briefly highlight the potential limitations of this approach.

Third-party data sharing involves the transmission of (first party) consumer-generated data from the app (second party) to an outside entity—the third party. Third-party data sharing occurs on multiple levels. For example, a health app developer may use a cloud-based service provider such as Amazon Web Services (AWS) to store a user's relevant health data—a core function of the app.[37] Meanwhile, other third-party tools make it easy to capture, remotely store, and review analytic data[38] or provide monetization via advertisements. In

33. Levy, *supra* note 16, at 686-87.

34. *See* Albert Fox Cahn & Eleni Manis, Surveillance Tech. Oversight Project, *Pregnancy Panopticon: Abortion Surveillance After Roe* 1–4 (2022), https://www.stopspying.org/s/202261_STOP-Report_Pregnancy-Panopticon.pdf.

35. Laura Shipp & Jorge Blasco, *How Private Is Your Period?: A Systematic Analysis of Menstrual App Privacy Policies*, 2020 PROC. ON PRIV. ENHANCING TECHS. 491, 494 (describing purposes for data collection, including operations, personalization, secondary use, scientific use, aggregation, and use by third parties).

36. For example, even if an app developer makes broad (and likely unrealistic) proclamations about how they would respond to requests from law enforcement, those promises do not matter if other, downstream parties have access to consumer data.

37. *See generally,* Amazon Web Services, Web and Mobile Apps https://aws.amazon.com/web-mobile-social/ (describing available services, including storage).

38. A typical use case for analytic data appears in the context of metrics. By collecting granular, time-series user interaction data (e.g., the sequence of button presses that a user makes to perform a given action), third-party analytics software development kits (SDKs) provide developers with the ability to "replay" exactly how a user interacts with the user interface or perform other advanced analyses, which provide valuable insights that allow for refinement of the app. *See generally, e.g.*, *What is Mixpanel?*, MIXPANEL, https://docs.mixpanel.com/docs/getting-started/what-is-mixpanel (last updated May 4, 2023) (describing a popular third-party analytics tool: "Mixpanel is an analytics tool that enables you to capture data on how users interact with your digital product. Mixpanel then lets you analyze this data with simple, interactive reports that let you query and visualize the data with just a few clicks."). While facilitating app improvements

each of these examples, the app is collecting and transmitting troves of data to third parties. Of course, these data are often useful—if not outright critical[39]—to the app developer's business purposes. But it also means that users' data comes into contact with entities that the user likely doesn't even know about, much less ones with whom they have contracted.

While many apps mention third-party data sharing in their privacy policies,[40] the details of what exactly happens to these data after they reach the developer's infrastructure are mostly unknowable from the outside. Absent a subpoena or the (often illicit) disclosure of source code, the machinations of the downstream infrastructure—any subsequent data transfers, cross-references, or inferences made from a user's data—are inscrutable[41] aside from what few guesses one may be able to make looking from the outside in. As a result, whether privacy policies are truthful is only partially knowable, and for most consumers, it comes down to trust.[42]

Fortunately, in most cases, it is possible to catch a glimpse into what an app is sending *before* it reaches the developer's servers by using a man-in-the-middle ("MITM") HTTP proxy server—essentially a modern-day variation of eavesdropping.[43] Instead of directly communicating with the remote servers, a specially configured smartphone (the client) routes its traffic through an intermediary server (the proxy server) controlled by an onlooker.[44] In turn, this proxy server intercepts communications sent back from the server and relays them back to the client smartphone.[45] From the perspectives of both the client and the server, it is business as normal: no

---

is certainly desirable, this frequent data collection can also sweep up sensitive information, which is problematic given that, unbeknownst to the end user, that sensitive information is either stored on (or at least passes through) third-party servers that are subject to different privacy policies.

39. For example, the date when one's period starts is a piece of data that is critical for a period tracking app to be able to function as advertised.

40. Blenner et. al., *supra* note 11, at 1051 tbl.1 (finding that, among a sample of 41 diabetes apps that provided privacy policies, 48.8% mentioned sharing data with third parties).

41. Huckvale et. al., *supra* note 25, at 2.

42. *Id.*

43. *Id.* at 3.

44. This configuration includes installing a custom-generated certificate of trust generated by the proxy server so that traffic that would otherwise be encrypted (and therefore unreadable) is instead legible to the proxy server.

45. *See* Huckvale et. al., *supra* note 25, at 3.

interruptions or other hints that anything is out of the ordinary. But in fact, there is a "man in the middle" spying on their communications, which is why this technique is most commonly associated with malicious actors.[46] When properly configured, the MITM proxy server can record (or potentially modify)[47] all communications that pass through, as well as any associated metadata.[48] Of course, the major downside to this technique is that not everyone can make use of it: Setting it up and being able to understand the results requires both time and a high level of background knowledge.

Put simply, apps make privacy promises to consumers using things like privacy policies, advertisements, and, on the App Store, the Privacy Label. However, whether these promises are true and complete is not guaranteed, and verifying requires significant technological know-how.

B. What Research Shows

While not common or reasonable for average consumers, researchers regularly use the "man-in-the-middle" approach described in Part IIA to assess whether an app's data-sharing practices match the terms described in an app's consumer-facing privacy claims.[49] Here, we focus on how a handful of studies of this nature have dealt with health apps—a category

---

46. This technique is commonly understood as a man-in-the-middle *attack*, which inheres a malicious connotation. *See man-in-the-middle attack (MitM)*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY: COMPUTER SECURITY RESOURCE CENTER, https://csrc.nist.gov/glossary/term/man_in_the_middle_attack (last visited June 9, 2023) (defining the term variously as "a form of active wiretapping attack" or "an attack").

47. *See Introduction*, MITMPROXY, https://docs.mitmproxy.org/stable/ (last visited Oct. 11, 2023) (advertising one popular tool's ability to "[i]ntercept HTTP & HTTPS requests and responses and modify them on the fly" and "[s]ave complete HTTP conversations for later replay and analysis"). This ability to spy on and modify communications is why a man-in-the-middle attack is typically undesirable. It is worth disclaiming that the use of a MITM attack for these purposes is intentional and requires deliberate use of unsafe security practices and specific bypassing of established safeguards.

48. Metadata is "data that provides information about other data." *Metadata*, MERRIAM-WEBSTER.COM, https://www.merriam-webster.com/dictionary/metadata (last visited Apr. 27, 2023). One common example of metadata is a called a "media type" (or "MIME type"), which signals to a receiving party which form the transmitted data will take (e.g., "image/jpeg", which signifies that the data being sent is an image and that it is a JPEG, or "text/html", which signifies that the data being sent is text that has been structured using the HyperText Markup Language).

49. *See, e.g.*, Huckvale et. al, *supra* note 25.

of technologies for which consumers may have heightened expectations of privacy and greater risks when those expectations do not match reality.

That technology companies—including health app developers—might obscure their data-sharing practices in privacy policies is likely unsurprising to anyone transacting in the modern digital economy. The disconnect between promises and practices contributes to the myriad issues with privacy policies, which are often derided as unread, unreadable, or completely unavailable.[50] And even if a consumer did endeavor to undertake the often herculean task of understanding these documents, they are frequently subject to unilateral amendment with little or no notice to consumers.[51] But setting aside the well-deserved critiques of the form and function of privacy policies, sometimes they simply lie: explicitly, by omission, or by obfuscation.

One prominent study on privacy risks for health and wellness apps dates back to 2015 when Huckvale et al. assessed 79 health and wellness apps certified as "clinically safe and trustworthy" by the United Kingdom's National Health Services (NHS) Health App Library.[52] After examining the content of privacy policies and capturing transmitted data,

50. Ali Sunyaev, Tobias Dehling, Patrick L. Taylor & Kenneth D. Mandl, *Availability and Quality of Mobile Health App Privacy Policies*, 22 J. AM. MED. INFORM. ASSOC. e28, e31 (2015) (finding that "privacy policies have poor availability rates, correlation of app ratings and privacy policy availability is weak, privacy policy scope is lacking, high [reading grade levels] are required to understand privacy policies, and privacy practices are not made transparent in a comprehensive fashion"); Nili Steinfeld, *"I Agree to the Terms and Conditions": (How) Do Users Read Privacy Policies Online? An Eye-Tracking Experiment*, 55 COMPUTS. IN HUM. BEHAV. 992, 993 (2016) (finding that when users can accept terms and conditions without reading them, they generally do not read them, and that users who spend more time looking at a policy will comprehend the terms better than those who do not); Leah R. Fowler, Charlotte Gillard & Stephanie R. Morain, *Readability and Accessibility of Terms of Service and Privacy Policies for Menstruation-Tracking Smartphone Applications*, 21 HEALTH PROMOTION PRAC. 679, 680-82 (2020) (finding that, in a sample of popular menstruation tracking apps, most terms of service and privacy policies fell short of recommended readability standards using readability statistics, some were impracticably long to read, and some were completely unavailable).

51. Leah R. Fowler, Jim Hawkins & Jessica L. Roberts, *Uncertain Terms*, 97 NOTRE DAME L. REV. 1, 4–5 (2021) (discussing unilateral amendment clauses in health app privacy policies that allow health tech companies to change their terms with little or no notification to consumers); Jessica L. Roberts & Jim Hawkins, *When Health Tech Companies Change Their Terms of Service*, 367 SCI. 745, 745 (2020).

52. Huckvale et. al., *supra* note 25, at 1.

the team showed that, among other findings, of the apps collecting or transmitting data, only 71% had a privacy policy.[53] In only 4% of these apps, information handling was completely consistent with the specified terms in the policy.[54] While the researchers did not find any apps in the sample that engaged in data sharing that directly contradicted privacy policies, 82% collected and 78% transmitted one or more data items not discussed in the privacy policy.[55] That a trusted entity in a position of authority—namely the NHS—held these apps out as trustworthy made the findings especially concerning.[56]

In 2019, Huckvale led a separate research team in a study that turned a critical eye toward smartphone apps for depression and smoking cessation.[57] The results here were similarly disappointing. Only 69% of studied apps had privacy policies.[58] Of those, only 88% described primary data uses, and even fewer (64%) described secondary uses.[59] Despite this, 92% of all studied apps transmitted data to one or more third parties, and of those that engaged in third-party data transmission, nine lacked a privacy policy, five failed to disclose this transmission in privacy policies, and three explicitly stated that this type of data transmission would not occur.[60] In their discussion, the authors specifically noted the negative implications of these findings for relying solely on self-certification of reviewing privacy policies to audit privacy protections.[61] Put bluntly, it could be a mistake to take these app developers at their word.

More recently, a 2022 analysis conducted by Koch et al. showed analogous deficiencies across categories of the App

53. *Id.* at 8.
54. *Id.*
55. *Id.*
56. This also happened in 2013, when Happtique suspended its health app certification program after a health IT firm exposed security risks of certified apps. *See* Brian Dolan, *Happtique suspends mobile health app certification program*, MOBILE HEALTH NEWS (Dec. 13, 2013) https://www.mobihealthnews.com/28165/happtique-suspends-mobile-health-app-certification-program/.
57. Kit Huckvale, John Torous & Mark E. Larsen, *Assessment of Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation,* J. AM. MED. ASSOC. NETWORK OPEN (2019).
58. *Id.*
59. *Id.*
60. *Id.*
61. *Id.*

Store with regard to Apple's Privacy Nutrition Labels.[62] Apple introduced these labels to their App Store in December 2020,[63] providing a succinct alternative to privacy policies that aspires to "help[] users better understand an app's privacy practices before they download the app."[64] Importantly, developers are the ones who choose what appears on the labels, not Apple or any other third party.[65] Koch et al. began by surveying 11,074 apps from the German App Store, finding that 48.87% of apps had no privacy label roughly one year after the labels' introduction.[66] Moreover, many of the apps that did have privacy labels had illogical declarations; for example, some declared collection of a user ID that is "not linked" to the user—an impossibility.[67] Koch et al. then collected and analyzed network traffic from a 1,687-app subset of the original 11,074 sample using a semi-automated, "man-in-the-middle" method.[68] By feeding in so-called "honey data"[69] and checking whether those bits of information subsequently appeared in collected traffic, the researchers could compare each app's actual transmissions with what it declared in its privacy label.[70] In total, Koch et al. found that 1,085 apps (64.66%) contacted at least one advertiser, 1,188 apps (70.80%) contacted at least one tracker, and 276 apps—just over 16% of the sample—transmitted data that were not listed in their privacy label.[71] Additionally, the researchers found that 282 apps transmitted unique, device-specific advertising

62. Simon Koch, et al., *Keeping Privacy Labels Honest*, 2022(4) PROC. ON PRIV. ENHANCING TECHS. 486, 492 (2022).

63. *App privacy labels now live on the App Store*, APPLE (last visited Dec. 14, 2020), https://developer.apple.com/news/?id=3wann9gh#:~:text=The%20App%20Store%20now%20helps,or%20used%20to%20track%20them.

64. *Id.*

65. *See App privacy details on the App Store*, APPLE, https://developer.apple.com/app-store/app-privacy-details (last visited May 19, 2023).

66. Simon Koch, et al., *Keeping Privacy Labels Honest*, 2022(4) PROC. ON PRIV. ENHANCING TECHS. 486, 492 (2022).

67. *Id.*

68. *Id.* at 495.

69. Koch et al. define "honey data" as items ranging from a user's location, calendar, and notes to hardware-specific items such as the operating system version and IMEI (a unique, hardware-tied device identifier). *See Koch et. al., supra* note 66, at 506 tbl.4 (2022).

70. *See* Koch et. al., *supra* note 66, at 497 (2022).

71. *See Id.* at 496-497.

identifiers, showing a "clear indicator of these apps' intent to track the user across apps and vendors."[72]

Taken together, these findings show that the privacy labels have not done much to improve on the privacy-policy model, and that despite all its overtures on privacy, Apple has done little to police the adoption, content, or accuracy of apps' privacy labels. Perhaps even more troubling is that these deficiencies persist even in a country subject to the General Data Protection Regulation (GDPR).[73]

III. MENSTRUAL DATA AFTER *DOBBS*

The problem we describe in Part II is present across technologies and raises unique concerns in health contexts given the sensitivity of the user data involved. However, these privacy misrepresentations could have particularly significant consequences for reproductive data in light of the retrenchment of reproductive rights taking place in the states after *Dobbs*.[74] In this Part, we explain the unique risks of menstruation tracking apps—a term we use interchangeably with period and fertility tracking apps—including the data they contain and how they can be used to effectuate civil and criminal laws intended to restrict abortion or protect the state's interest in fetal health. We then turn to what the

72. This identifier is known as IDFA (Identifier For Advertisers) and has largely been obviated as of iOS 14.5 because Apple has turned it off by default, instead requiring explicit consent. Still, the means for retrieving the IDFA remains available, and as Koch et al. show, many apps clearly continue to request it in the hopes that some users have allowed access to it. *See* Simon Koch, Malte Wessels, Benjamin Altpeter, Madita Olvermann & Martin Johns, *Keeping Privacy Labels Honest*, 2022(4) PROC. ON PRIV. ENHANCING TECHS. 486, 496 (2022).

73. *See* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, 88 (declaring that "[the GDPR] shall be binding in its entirety and directly applicable in all Member States"); *see also Germany*, EUROPEAN UNION, https://european-union.europa.eu/principles-countries-history/country-profiles/germany_en (last visited June 9, 2023) (noting that Germany has been an EU member country since January 1, 1958).

74. *See, e.g.*, Elizabeth Nash & Isabel Guarnieri, *Six Months Post-Roe, 24 US States Have Banned Abortion or Are Likely to Do So: A Roundup*, GUTTMACHER INSTITUTE (Jan. 10, 2023), https://www.guttmacher.org/2023/01/six-months-post-roe-24-us-states-have-banned-abortion-or-are-likely-do-so-roundup.

empirical literature tells us about how prevalent the types of data deceptions we identify in Part II may be in this context.

A. Period and Fertility Tracking Apps

In the age of smartphones, nearly everyone carries a calendar in their pocket, and accordingly, applications designed to ease tracking periods using calendar-based methods have become a popular product category. Typing "period tracker" into the search bar in both the Apple App Store and the Google Play Store returns dozens of results.[75] As much as one-third of menstruating Americans in the 18-and-over category use such an app—as many as 39 million users as of 2019.[76] From a business perspective, this is no wonder: According to a 2019 report, the market size for women's health apps is expected to reach $3.9 billion by 2026.[77] In short, there is a massive market for menstruation trackers, and developers are seizing the opportunity.

Invariably, menstruation trackers do exactly what the name suggests: they track the user's menstrual period. However, they vary quite a bit in their intended uses. Any given menstruation tracker's offerings can range from what is essentially no more than a calendar-based diary[78] all the way up to a full-fledged fertility predictor, incorporating data such

---

75. Based on our own search of the term "period tracker" in the web-based versions of both the Apple App Store and the Google Play Store as of April 14, 2023.

76. *Health Apps and Information Survey September 2019*, *KAISER* FAM. FOUND., HEALTH APPS & INFO. SURV. 5 (2019), https://files.kff.org/attachment/Topline-Health-Apps-and-Information-Survey-September-2019; The U.S. Census Bureau estimated that there were 130,851,717 females 18 and over in the United States in July 2019. Population Division, *Annual Estimates of the Resident Population for Selected Age Groups by Sex for the United States: April 1, 2010 to July 1, 2019*, U.S. CENSUS BUREAU, https://www2.census.gov/programs-surveys/popest/tables/2010-2019/national/asrh/nc-est2019-syasexn.xlsx [https://web.archive.org/web/20220728102007/https://www2.census.gov/programs-surveys/popest/tables/2010-2019/national/asrh/nc-est2019-syasexn.xlsx] (last visited Nov. 3, 2022). Thirty percent of 130,851,717 is 39,255,515 (rounded down). Therefore, as many as ~39.25 million women used period tracker apps as of July–September 2019.

77. *Women's Health App Market Worth $3.9 Billion by 2026*, BLOOMBERG (Dec. 5, 2019), https://www.bloomberg.com/press-releases/2019-12-05/women-s-health-app-market-worth-3-9-billion-by-2026-cagr-17-9-grand-view-research-inc.

78. *Spot On Period Tracker*, PLANNED PARENTHOOD, https://www.plannedparenthood.org/get-care/spot-on-period-tracker (last visited Nov. 3, 2022).

as basal body temperature.[79] Some even integrate sharing features, ostensibly to keep the user's partner in the loop or to "[s]ync cycles with . . . friends,"[80] while others claim to "Sync [your cycle] with the moon."[81]

The amounts and different types of data that menstruation trackers collect are related to the range of intended uses. But one thread links all of them: This data is some of the most personal information their users can provide. One stereotypical example to examine is *Period Tracker Period Calendar* ("PTPC"), developed by ABISHKKING LIMITED.[82] The app appears quite popular; it shows up near the top of search results on the Apple App Store, has (at a minimum) hundreds of thousands of downloads,[83] and boasts of a userbase of "over 300,000,000 women across 45+ countries."[84] PTPC is a veritable Swiss Army knife of an app, offering a "period & cycle calendar," an "ovulation & fertility tracker," a week-by-week pregnancy tracker, a "birth control planner," a "pill reminder," and "symptom prediction & tips."[85] To provide this laundry list of features, PTPC collects a mountain of different data points ranging from the mundane—hydration, sleep, mood, and number of steps—to the highly private—cervical mucus viscosity, birth control methods, period flow intensity, and sex

79. *How does Natural Cycles work?*, NAT. CYCLES, https://www.naturalcycles.com/how-does-natural-cycles-work (last visited Nov. 3, 2022).

80. CYCLES, https://cycles.app (last visited Nov. 3, 2022) ("A Cycle Built for Two: . . . Invite your partner to follow your cycle"); STARDUST, https://stardust.app (last visited Nov. 3, 2022) ("Sync cycles with your friends.").

81. STARDUST, https://stardust.app (last visited Nov. 3, 2022).

82. *Period Tracker Period Calendar*, APPLE APP STORE PREVIEW, https://apps.apple.com/us/app/period-tracker-period-calendar/id896501514 (last visited Nov. 12, 2022).

83. The true number of downloads for any given app on the App Store is unknown for members of the public because Apple does not make such data publicly available. However, one (albeit imperfect) proxy for app download numbers is the number of ratings for a given app. As of May 2023, Period Tracker Period Calendar had over 126,000 ratings on the United States version of the App Store. *Period Tracker Period Calendar*, APPLE APP STORE PREVIEW, https://apps.apple.com/us/app/period-tracker-period-calendar/id896501514 (last visited May 22, 2023). Assuming that most raters have also downloaded the app at some point and that the number of ratings is necessarily smaller than the number of downloads, then the number of downloads for Period Tracker Period Calendar must be well into the hundreds of thousands.

84. *See Period Tracker Period Calendar*, APPLE APP STORE PREVIEW, https://apps.apple.com/us/app/period-tracker-period-calendar/id896501514 (last visited Nov. 12, 2022).

85. *Id.*

(even including whether the user had an orgasm).[86] Though PTPC's week-by-week pregnancy tracker is not exactly common amongst its peers, its core feature of period and ovulation tracking and the attendant data behind it is the bread and butter of all menstruation trackers.

From an economic perspective, there is a misalignment between the incentives of the menstruation tracker developers and those of the users—particularly for apps that are free of charge that comprise the majority of the market. It is fair to assume that the primary incentive of menstruation tracker developers, as is the case with almost any business, is to make a profit.[87] Expending all the effort to design, build, market, distribute, and maintain an app must net the developer some reward, after all. Similarly, one can reasonably assume that the users' primary incentive is to derive a health benefit from the app, either by successfully getting pregnant, avoiding conception, or otherwise staying informed about an important part of their overall health—which necessarily incentivizes turning over as much personal data as possible. The developers' goal of earning a profit can come at the direct expense of the privacy of users' personal health information because the developer likely does not earn money unless they provide that data (or access to it) to a third party.

While this economic paradigm of data sharing is prevalent and problematic across consumer technologies, sharing menstrual data raises additional concerns. While the relevance of menstrual data for legal and political purposes existed well before the fall of *Roe v. Wade,*[88] the rapidly evolving post-*Dobbs*

86. Sadaf Khan, *Data Bleeding Everywhere: A Story of Period Trackers,* DEEP DIVES (June 7, 2019), https://deepdives.in/data-bleeding-everywhere-a-story-of-period-trackers-8766dc6a1e00.

87. In the case of the overwhelming majority of menstruation trackers, developers make their money through offering an increased feature set with a paid subscription, selling their users' information to third parties, or a combination of the two.

88. Yasmeen Abutaleb & Emily Wax-Thibodeaux, *Missouri Reviewed Data About Planned Parenthood's Patients, Including Their Periods, to Identify Failed Abortions,* WASH. POST (Oct. 30, 2019 6:15 PM EDT), https://www.washingtonpost.com/health/missouri-tracked-planned-parenthood-patients-periods-in-spreadsheet-top-health-official-says/2019/10/30/e96791d0-fb42-11e9-ac8c-8eced29ca6ef_story.html (reporting on a state hearing in which Missouri's state health director described monitoring health records from Planned Parenthood patients—including reviewing dates of last menstrual cycles); Jennifer Wright, Opinion, *The U.S. Is Tracking Migrant Girls' Periods to Stop Them from Getting Abortions*, HARPER'S BAZAAR (Apr. 2, 2019)

legal landscape creates new risks for these data. For example, a state interested in limiting abortion access to those at or before six weeks of gestation[89] must identify the date of a user's last menstrual period to determine gestational age.[90] States interested in prosecuting citizens for abortions that took place out-of-state[91] may be interested in menstrual data that shows a period that did not come when expected and then later resumed after traveling to a state with legal abortion. And if states pursue fetal personhood[92] and seek to protect their interest in the fetus at "all stages of development,"[93] data that speaks to whether a consumer knew or should have known of a pregnancy may be relevant to building a case.[94] These data points exist in all menstruation trackers. That these data are poor evidence of wrongdoing[95] may not be a deterrent to motivated actors.[96] And given the ever-evolving legal

---

https://www.harpersbazaar.com/culture/politics/a26985261/trump-administration-abortion-period-tracking-migrant-women (detailing the tracking of migrant reproductive health information, including menstruation).

89. *See e.g.*, S.B. 8, 87th Leg., Reg. Sess. (Tex. 2021) (codified at TEX. HEALTH & SAFETY §§ 171.203(b), 171.204(a)).

90. Last menstrual period or "LMP" is traditionally used to calculate estimated due date and gestational age. ACOG Methods for Estimating the Due Date. *Methods for Estimating the Due Date*, The American College of Obstetricians and Gynecologists, Committee Opinion No. 700 (2017).

91. Alice Miranda Ollstein & Megan Messerly, *Missouri Wants to Stop Out-Of-State Abortions. Other States Could Follow.*, POLITICO (Mar. 19, 2022, 7:00 AM EDT), https://www.politico.com/news/2022/03/19/travel-abortion-law-missouri-00018539.

92. *See e.g.*, S.B. 1457, 55th Leg., 1st Reg. Sess. (Ariz. 2021) (codified at ARIZ. REV. STAT. ANN. § 1-219(A)) (granting an "unborn child at every stage of development, all rights, privileges and immunities available to other persons, citizens, and residents"). This law is currently being challenged in *Isaacson v. Brnovich*, No. CV-21-01417-PHX-DLR, 2022 WL 2665932, at *1, *10 (D. Ariz. July 11, 2022). *See also* H.B. 704, 134th Gen. Assemb., Reg. Sess. (Ohio 2022). Both the Arizona and Ohio laws would recognize fetuses as legal persons from the moment of conception and afford them the same constitutional rights as born persons.

93. In its recounting of historical abortion regulations, the *Dobbs* opinion makes special note of the application to "all stages" at least thirteen times. *See, e.g.,* Dobbs, *supra* note 1.

94. Leah R. Fowler & Michael R. Ulrich, *Femtechnodystopia,* 75 STAN. L. REV. 1233, 1274–1276 (2023).

95. Kendra Albert, Maggie Delano & Emma Weil, *Okay, Fine, Let's Talk About Period Tracking: The Detailed Explainer*, MEDIUM (June 28, 2022), https://medium.com/@maggied/okay-fine-lets-talk-about-period-tracking-the-detailed-explainer-2f45112eebb4.

96. *See generally* Valena E. Beety & Jennifer D. Oliva, *Policing Pregnancy "Crimes,"* 98 NYU L. REV. ONLINE 29 (2023).

landscape, we do not claim that this list of potential data uses is exhaustive.

B. What Research Shows About Menstrual Data

One might be inclined to believe that because of the intensely intimate nature of menstrual data, the information these apps contain is entitled to special protections under the law. However, as a general matter, they are not treated differently than other types of data in the ways we typically expect.[97] Some select states,[98] as well as the FTC's recent approach to its Health Breach Notification Rule,[99] certainly acknowledge consumer health data are different from other categories of data. But typically, no special protections apply to sensitive health data in a consumer health technology context. Some states and the federal government have even tried—and failed—to pass legislation specific to reproductive data.[100] However, generally speaking, consumer data is simply treated as consumer data regardless of how intimate it is.

As a result, whether app developers treat menstrual data with additional care is largely discretionary. Much like the studies described in Part II, whether app developers respect the sensitive nature of the data in period and fertility tracking

---

97. For example, HIPAA does not apply to the vast majority of apps. OFFICE FOR CIV. RTS., *Protecting the Privacy and Security of Your Health Information When Using Your Personal Cell Phone or Tablet*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html (last visited Jan. 28, 2023). ("In most cases, unless the app is provided to you by a covered entity or its business associate, the HIPAA Rules also do not protect the privacy of data you've downloaded or entered into mobile apps for your personal use, regardless of where the information came from.").

98. *E.g.*, California Consumer Privacy Act, CAL. CIV. CODE § 1798.140(ae)(2)(B) (defining "sensitive personal information" to include "[p]ersonal information collected and analyzed concerning a consumer's health"); Washington My Health My Data Act § 3(8)(a), 2023 Wash. Sess. Laws 191 (to be codified at WASH. REV. CODE § 19.44.28) (defining "consumer health data" as "personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status.").

99. *See* Complaint for Permanent Injunction, Civ. Penalty Judgment, and Other Relief at 18–21, United States v. Easy Healthcare Corp., No. 1:23-cv-03107 (N.D. Ill. May 17, 2023); *Complying with the FTC's Health Breach Notification Rule*, FTC (Jan. 2022), https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule.

100. *See, e.g.*, My Body, My Data Act of 2022, H.R. 8111, 117th Cong. (2022); *see also* S.B. 852, 2023 Reg. Sess. (Va. 2023).

apps and treat it differently of their own accord has been the subject of recent scrutiny. In 2022, Alfawzan et al. conducted a scoping review and content analysis to assess various privacy considerations in femtech apps[101]—including, but not limited to, fertility, ovulation, or menstrual cycle tracking.[102] They found that privacy policies were inconsistently available and of varying quality and comprehensiveness.[103] Based on an assessment of these policies, the researchers observed that, of the 23 apps included in their sample, "20 (87%) shared user data with third parties, 9 (39%) did not require explicit consent to share user data with third parties, and 3 (13%) did not provide any information in their privacy policies and did not require consent related to the sharing of user data with third parties."[104]

But, importantly, Alfawzan et al. presented what their sample app developers *tell* consumers, not what they do. Recall from Part II that it is inadvisable, as a general matter, to take an app developer at its word.[105] One must ask different research questions to understand how their words and their actions might differ. In their 2021 work, Mehrnezhad and Almeida probed the potential disconnect by evaluating privacy notices compared to tracking practices.[106] Their study noted that most fertility apps in the sample had trackers and, on

101. "Femtech" is a catch-all industry term for an enormous category of products targeting "female" health. Ida Tin, *The Rise of a New Category: Femtech*, CLUE (Sept. 14, 2016), https://helloclue.com/articles/culture/rise-new-category-femtech. The "fem" in "femtech" is from the word "female," though this paper uses inclusive language wherever possible. People who menstruate and are capable of becoming pregnant includes "women, transgender males, intersex persons, [non-]binary persons, and other persons who have the capacity for a menstrual cycle." Margaret E. Johnson, *Menstrual Justice*, 53 U.C. DAVIS L. REV. 1, 5 n.6 (2019). A 2021 survey revealed that, of people engaging in digital period tracking, "19% of menstruating respondents identified as men, 24% of which reported digitally tracking their periods." Ashwini Nagappan, et al., *To Track or Not to Track? How Digital Period Tracking May Change in a Post-*Dobbs *World*, ROCK HEALTH (Aug. 29, 2022), https://rockhealth.com/insights/to-track-or-not-to-track-how-digital-period-tracking-may-change-in-a-post-dobbs-world/.

102. Najd Alfawzan, et al., *Privacy, Data Sharing, and Data Security Policies of Women's mHealth Apps: Scoping Review and Content Analysis,* J. MED. INTERNET RES. MHEALTH UHEALTH 197, 200 (2022).

103. *Id.*

104. *Id.*

105. *Supra* Part II.A.2.

106. Maryam Mehrnezhad & Teresa Almeida, *Caring for Intimate Data in Fertility Technologies*, 2021 PROC. CHI CONF. ON HUM. FACTORS IN COMPUTING SYS. 1, 6 (2021).

average, had more trackers than had been observed in other studies of popular general websites.[107] By contrast, Shipp and Blasco observed that period and fertility tracking apps perform slightly better than other health-related or general apps when it comes to privacy practices.[108] Notwithstanding that bit of optimism, they still observed that privacy policies often fall short of clearly communicating data-sharing practices, especially as it pertains to third parties.[109] And many developers do not contemplate the sensitive nature of menstrual and reproductive data in their privacy policies at all.[110]

III. MEASURED PROGRESS

The behaviors described in Parts II and III—where a developer claims to provide certain data protections but does not—are already broadly illegal[111] regardless of whether it implicates reproductive data. And given that existing laws and regulations already prohibit[112] these false or deceptive acts or practices, it is worth reflecting on how and why they can work and where they fall short in light of resource limitations and the peculiarities of the marketplace. In this Part, we describe how existing mechanisms can—and sometimes do—hold companies to the privacy promises they make to consumers, including some highlights of new privacy legislation emerging

107. *Id.*

108. Laura Shipp & Jorge Blasco, *How Private Is Your Period?: A Systematic Analysis of Menstrual App Privacy Policies*, 2020 PROC. ON PRIV. ENHANCING TECHS. 491, 503 (2020).

109. Mehrnezhad & Almeida, *supra* note 106, at 6 (finding that only 5 privacy policies [16% of the sample] explicitly mentioned the third party libraries embedded within the app and specified the kind of data sent to those libraries).

110. Shipp & Blasco, *supra* note 108, at 504–505.

111. *See, e.g.*, Complaint for Permanent Injunction, Civ. Penalty Judgment, and Other Relief, United States v. Easy Healthcare Corp., No. 1:23-cv-03107 (N.D. Ill. May 17, 2023) (FTC action against an app developer for deceptive privacy claims); *In re* Flo Health, Inc., Docket No. C-4747, FTC Matter No. 1923133 (June 2021) (complaint), https://www.ftc.gov/system/files/documents/cases/192_3133_flo_health_complaint.pdf (another FTC action against a different app developer for deceptive privacy claims).

112. *See, e.g.*, Complaint for Permanent Injunction, Civ. Penalty Judgment, and Other Relief, United States v. Easy Healthcare Corp., No. 1:23-cv-03107 (N.D. Ill. May 17, 2023) (FTC action against an app developer for deceptive privacy claims); *In re* Flo Health, Inc., Docket No. C-4747, FTC Matter No. 1923133 (June 2021) (complaint), https://www.ftc.gov/system/files/documents/cases/192_3133_flo_health_complaint.pdf.

post-*Dobbs*. We then turn to where these approaches can still fall short when it comes to the privacy misrepresentations we contemplate in this paper, as well as some temporary measures to help augment state and federal approaches in the near term.

A. Some Limited Successes

Currently, the types of laws and regulations that prevent these behaviors generally fall into the category of consumer protection from false or deceptive acts or practices—usually under state deceptive trade practice acts or the broad powers of the FTC.[113] Such practices could also be violations of specific state privacy laws where they are present. We briefly consider some benefits and incremental progress of each.

All fifty states have laws that address unfair or deceptive acts and practices;[114] however, they vary in their structure, priorities, and available resources.[115] At the federal level, the FTC is perhaps the most active force in this space. Congress has empowered the FTC to prevent "persons, partnerships, or corporations" from using "unfair or deceptive acts or practices in or affecting commerce."[116] Its powers are broad, and extend to ensuring that claims in advertising are "truthful, cannot be deceptive or unfair, and must be evidence-based."[117] The

113. *See, e.g.*, Consumer *Protection in the States, a 50-State Evaluation of Unfair and Deceptive Practice Laws*, NAT'L CONSUMER L. CTR., (Mar. 2018) https://www.nclc.org/wp-content/uploads/2022/09/UDAP_rpt.pdf (explaining state-level deceptive trade practices); Complaint for Permanent Injunction, Civ. Penalty Judgment, and Other Relief, United States v. Easy Healthcare Corp., No. 1:23-cv-03107 (N.D. Ill. May 17, 2023) (FTC action against an app developer for deceptive privacy claims); *In re* Flo Health, Inc., Docket No. C-4747, FTC Matter No. 1923133 (June 2021) (complaint), https://www.ftc.gov/system/files/documents/cases/192_3133_flo_health_complaint.pdf (another FTC action against a different app developer for deceptive privacy claims).

114. *Consumer Protection in the States, a 50-State Evaluation of Unfair and Deceptive Practice Laws*, NAT'L CONSUMER L. CTR., (Mar. 2018) https://www.nclc.org/wp-content/uploads/2022/09/UDAP_rpt.pdf (presenting the results of a 50-state survey evaluating the strengths and weaknesses of unfair and deceptive acts and practices laws).

115. *Id*.

116. 15 U.S.C. § 45(a)(2) (empowering and directing FTC to prevent persons, partnerships, or corporations from using unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce).

117. U.S. FED. TRADE COMM'N, Advertising and Marketing Basics, https://www.ftc.gov/businessguidance/advertising-marketing/advertising-marketing-basics (last visited May 9, 2021).

agency can exert this authority by suing[118] or bringing enforcement actions against corporations that make deceptive claims, including those involving the use and protection of user data.[119]

The FTC has leveraged this power in the realm of period and fertility tracking privacy targeting the types of behavior we discuss in this paper. In 2023, the FTC brought a case against Easy Healthcare Corporation, developer of a period and fertility tracking app called Premom, for breaking privacy promises to consumers.[120] Easy Healthcare allegedly used third-party tools called software development kits (SDKs) that gathered analytics and advertising data paired with unique identifiers.[121] According to the FTC's complaint, these data were disclosed via descriptive "custom app events," which were used to track users' interactions with the app.[122] But these custom app events also exfiltrated menstruation, fertility, and pregnancy information to third parties.[123] By allowing third parties to gather these custom app events, Easy Healthcare allegedly violated its promises that it would not share health information with third parties without its users' knowledge or consent.[124] The FTC also alleged that Easy Healthcare did nothing to limit what these third-party companies could later do with the health data they obtained.[125] In a novel strategy compared to similar prior actions[126] but consistent with more recent approaches,[127] the FTC also alleged that Easy

118. *See, e.g.,* Complaint for Permanent Injunction & Other Relief, Federal Trade Commission v. Kochava, Inc., No. 22-cv-377, 2022 WL 4080538 (D. Idaho Aug. 29, 2022).

119. *See* Complaint, *In re* Flo Health, Inc., Docket No. C-4747, FTC Matter No. 1923133 (June 2021) https://www.ftc.gov/system/files/documents/cases/192_3133_flo_health_complaint.pdf.

120. *See* Complaint for Permanent Injunction, Civ. Penalty Judgment, and Other Relief at 2–4, United States v. Easy Healthcare Corp., No. 1:23-cv-03107 (N.D. Ill. May 17, 2023).

121. *Id.* at 8-15.

122. *Id.* at 8-9.

123. *Id.* at 9.

124. *Id.* at 9.

125. *Id.* at 3, 15-18.

126. *C.f.* In the Matter of Flo Health, Inc., FTC File No. 1923133 (June 22, 2021), https://www.ftc.gov/system/files/documents/cases/flo_health_complaint.pdf.

127. FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising, FEDERAL TRADE COMMISSION (Feb. 1, 2023) https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-

Healthcare's non-consensual sharing of its users' health information amounted to a "breach of security" and, thus, a violation of the Health Breach Notification Rule (HBNR).[128] Alongside the complaint was a proposed, stipulated consent decree, indicating Easy Healthcare's intent to settle the matter.[129] The proposed order would see Easy Healthcare pay a $100,000 civil penalty for violating the HBNR and permanently enjoin the company from sharing personal health data with third parties, among many other remedial requirements.[130] The FTC also separately announced that Easy Healthcare would pay an additional $100,000 to Connecticut, the District of Columbia, and Oregon for violations of their respective laws.[131]

Importantly, the primary issue in this case was not necessarily that the app shared health data. As described above, period and fertility tracking apps share data all the time, and data sharing itself is not illegal.[132] The problem was that they allegedly broke promises they made to consumers. If a hypothetical company in a similar position did the same thing but used different language to describe its third-party data-sharing with consumers truthfully and obtained their consent, this type of data-sharing would likely be perfectly legal.[133]

---

enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising.

128. Complaint for Permanent Injunction, Civ. Penalty Judgment, and Other Relief at 18–21, United States v. Easy Healthcare Corp., No. 1:23-cv-03107 (N.D. Ill. May 17, 2023).

129. Stipulated Ord. for Permanent Injunction, Civ. Penalty Judgment, and Other Relief, United States v. Easy Healthcare Corp., No. 1:23-cv-03107 (N.D. Ill. May 17, 2023).

130. *See* Stipulated Ord. for Permanent Injunction, Civ. Penalty Judgment, and Other Relief, United States v. Easy Healthcare Corp., No. 1:23-cv-03107 (N.D. Ill. May 17, 2023); *Ovulation Tracking App Premom Will be Barred from Sharing Health Data for Advertising Under Proposed FTC Order*, U.S. FED. TRADE COMM'N (May 17, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc?utm_source=govdelivery.

131. *Ovulation Tracking App Premom Will be Barred from Sharing Health Data for Advertising Under Proposed FTC Order*, U.S. FED. TRADE COMM'N (May 17, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc?utm_source=govdelivery.

132. *Supra* Part II.B.

133. Leah R. Fowler, Jim Hawkins & Jessica L. Roberts, *Uncertain Terms*, 97 NOTRE DAME L. REV. 1, 1 (2021).

The permissibility of reproductive data sharing given the right conditions is one place where specific privacy laws can fulfill different roles than more generalized consumer protection approaches by prohibiting or limiting what data a company can collect, store, sell, and share. Unfortunately, the United States lacks a robust national privacy law akin to the European Union's GDPR.[134] Instead, most privacy laws appear at the state level.[135] As of October 2023, thirteen states have enacted their own data privacy schemes.[136] Even though some are quite comprehensive, they often only extend to the states' jurisdictions, necessarily excluding large swaths of those affected by privacy violations.[137] What's more, the various schemes vary widely in terms of their applicability, coverage, and enforcement.

---

134. *See generally* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

135. *See e.g.,* See Stacey A. Tovino, *Going Rogue: Mobile Research Applications and the Right to Privacy*, 95 NOTRE DAME L. REV. 155, 190–206 (2019) (presenting the results of a 50-state survey describing privacy laws with potential applicability to mobile-app mediated research conducted by independent scientists).

136. *A Comprehensive Resource for Tracking U.S. State Consumer Data Privacy Legislation*, HUSCH BLACKWELL, https://www.huschblackwell.com/2023-state-privacy-law-tracker (last updated Sept. 12, 2023).

137. *But see ACLU v. Clearview AI, Inc.*, 2020 CH 04353 (Cir. Ct. Cook Cty., Ill.) (a lawsuit in which plaintiffs sued Clearview AI for violating the Illinois Biometric Information Privacy Act, resulting in a settlement that banned Clearview AI from making its faceprint database available to most businesses and other private actors. The ban is applicable nationwide). May 4, 2022 Settlement Agreement available at https://www.aclu.org/legal-document/exhibit-2-signed-settlement-agreement?redirect=exhibit-2-signed-settlement-agreement. Of course, Clearview is offering other facial recognition products not covered by the settlement. *See, e.g.*, *Clearview AI Launches Clearview Consent; Company's First Consent Based Product for Commercial Uses*, BUSINESSWIRE (May 25, 2022 06:36 AM Eastern Daylight Time), https://www.businesswire.com/news/home/20220525005378/en/Clearview-AI-Launches-Clearview-Consent-Company%E2%80%99s-First-Consent-Based-Product-for-Commercial-Uses. Further, some settlements with state agencies also have nationwide reach. *See* Michelle M. Mello, Trish Riley & Rachel E. Sachs, *The Role of State Attorneys General in Improving Prescription Drug Affordability*, 95 S. CAL. L. REV. 595, 607–09 (2022) (describing how state attorneys general can influence national public health policy—including setting national regulatory systems for companies without legislative or federal involvement—through settlement agreements, and noting that attorneys general can often achieve outcomes in settlement that would not be possible in the actual lawsuit).

One recent post-*Dobbs* example comes from Washington. Signed into law on April 27, 2023, the Washington My Health My Data Act focuses specifically on consumer health data.[138] The prime sponsor of the bill is on record as saying that it was at least partially motivated by both the *Dobbs* decision as well as the dangers associated with period tracking apps selling sensitive information about women's reproductive health.[139] All things considered, this law is well-rounded and empowering for consumers. Importantly, this statute applies to anyone who does business in Washington, small or large[140]—not just the big players.[141] Under this law, consumers have the right to confirm collection, sharing, or selling of their health data and to access their data;[142] the right to withdraw consent from the collection and sharing of their health data;[143] and the right to delete their health data.[144] It also grants consumers a

138. Washington My Health My Data Act, 2023 Wash. Sess. Laws 191 (to be codified at WASH. REV. CODE § 19.44.28).

139. *See Addressing the collection, sharing, and selling of consumer health data: Hearing on HB 1155*, 68th Leg., 2023 Reg. Sess. at 07:36, 08:00 (Jan. 24, 2023) (statement of Rep. Vandana Slatter), https://tvw.org/video/house-civil-rights-judiciary-2023011514/?eventID=2023011514.

140. The statute covers "regulated entities," which is defined broadly as any legal entity that "[c]onducts business in Washington, or produces or provides products or services that are targeted to consumers in Washington" and who "determines the purpose and means of collecting, processing, sharing, or selling of consumer health data." Washington My Health My Data Act § 3(23)(a)–(b), 2023 Wash. Sess. Laws 191 (to be codified at WASH. REV. CODE § 19.44.28). The statute goes on to define "small business" so as to cover even the smallest businesses that handle consumer health data. *See* Washington My Health My Data Act § 3(28)(a)–(b), 2023 Wash. Sess. Laws 191 (to be codified at WASH. REV. CODE § 19.44.28).

141. For example, California's Consumer Privacy Act, one of the most sweeping state-level consumer privacy schemes in the country, sets a fairly high threshold before a business must adhere to its consumer privacy laws. *See* California Consumer Privacy Act, CAL. CIV. CODE § 1798.140(d) (defining "business" as (a) a legal entity that had annual gross revenues in excess of $25,000,000, (b) annually handles the personal information of 100,000 or more consumers or households, or (c) derives 50 percent or more of its annual revenues from selling or sharing consumers' personal information). This definition necessarily excludes the hypothetical smaller app developer who may not see "100,000 or more" users but who nevertheless deals with tens of thousands of users' personal information.

142. Washington My Health My Data Act § 6(1)(a), 2023 Wash. Sess. Laws 191 (to be codified at WASH. REV. CODE § 19.44.28).

143. Washington My Health My Data Act § 6(1)(b), 2023 Wash. Sess. Laws 191 (to be codified at WASH. REV. CODE § 19.44.28).

144. Washington My Health My Data Act § 6(1)(c), 2023 Wash. Sess. Laws 191 (to be codified at WASH. REV. CODE § 19.44.28).

private right of action by way of incorporating by reference Washington's unfair and deceptive trade practices law,[145] which permits seeking injunctive relief as well as actual damages, court costs, attorneys' fees, and even treble damages where appropriate.[146] One standout provision is the explicit prohibition on geofences[147] surrounding in-person healthcare facilities that are used to track, collect data about, or serve advertisements to consumers,[148] which is a problem that even the FTC has had trouble prosecuting.[149] This proscription is particularly beneficial for those who come to Washington from abortion-hostile states to seek abortions.[150] Those hostile states' ability to prosecute falters if the businesses that would otherwise provide them with evidence that ties an individual to an abortion provider cannot collect that evidence in the first place. Nevertheless, despite all its promise, the law remains untested because it is so new, phasing into effect on July 23, 2023.[151]

B. One of Many Remaining Challenges

Despite limited successes, we believe existing and newly introduced laws and regulations will continue to struggle to keep pace with the expansive market for consumer health technologies. Here, we return to our paper's central problem of privacy lies and identify small, collaborative steps that can

145. Washington My Health My Data Act § 11, 2023 Wash. Sess. Laws 191 (to be codified at WASH. REV. CODE § 19.44.28); *see generally*, WASH. REV. CODE § 19.86.010–.920 (Washington's unfair and deceptive trade practices statutes).

146. WASH. REV. CODE § 19.86.090.

147. The statute defines a geofence as "technology that uses global positioning coordinates, cell tower connectivity, cellular data, radio frequency identification, Wifi data, and/or any other form of spatial or location detection to establish a virtual boundary around a specific physical location, or to locate a consumer within a virtual boundary." Washington My Health My Data Act § 3(14), 2023 Wash. Sess. Laws 191 (to be codified at WASH. REV. CODE § 19.44.28).

148. Washington My Health My Data Act § 10, 2023 Wash. Sess. Laws 191 (to be codified at WASH. REV. CODE § 19.44.28).

149. *See, e.g.*, Federal Trade Commission v. Kochava, Inc., No. 2:22-cv-00377, 2023 WL 3249809, at *1 (D. Idaho May 4, 2023) (granting defendant data broker's 12(b)(6) motion to dismiss in a lawsuit in which the FTC alleged that the data broker's sale of geolocation data paired with unique identifiers, especially with regard to "sensitive locations," violated consumers' privacy and exposed them to risks of secondary harm).

150. *See* Ollstein & Messerly, *supra* note 91.

151. Washington My Health My Data Act, 2023 Wash. Sess. Laws 191 (to be codified at WASH. REV. CODE § 19.44.28).

help augment government efforts. In it, we emphasize that if we cannot hold companies to the privacy promises they make to consumers, any regulatory or legislative victories—no matter how comprehensive—will be insufficient.

A contributing factor to privacy and consumer protection laws alike is the relative staffing and resources of those tasked with enforcement compared to the large and dynamic market for consumer technologies. For example, the FTC has limited resources and must work carefully to target the largest players and the most egregious behaviors to maximize impact.[152] But app stores offer thousands of health apps, of which dozens are period and fertility trackers. The developers of these period tracker apps are a mixed bag of various corporations, LLCs, and even individuals.[153] Some apps have enjoyed millions of downloads, while others are less popular but nevertheless impact at least some consumers. As a result, while a select few offenders may invite scrutiny, smaller apps are likely to fly under the radar.

Recall from Part IIA that there is a high threshold of knowledge required to uncover these types of behaviors, regardless of the size and popularity of an app. Knowing the ins and outs of how and why apps communicate with their backend infrastructure represents a baseline level of knowledge that most people already do not possess, much less understanding how to eavesdrop on and comprehend these communications. And on top of all of this, it takes a fair amount of time to perform these checks on even one app, much less each one of the dozens of apps that consumers could consider when looking for a menstrual tracking app. Though government agencies may be in a better position to achieve this on a technical level, the sheer volume of apps on the market—each with its own particular set of privacy promises—makes

152. FED. TRADE COMM'N, FTC REPORT TO CONGRESS ON PRIVACY AND SECURITY 3–6 (2021), https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf (describing the FTC's priorities in privacy and security and noting that they "focus most of [their] limited resources on the most egregious practices and cases against major players in the marketplace in order to have a broader impact").

153. *See* Laura Shipp & Jorge Blasco, *How Private is Your Period?: A Systematic Analysis of Menstrual App Privacy Polices*, 2020(4) PROC. ON PRIV. ENHANCING TECHS. 496, tbl.1 (2020).

adequate oversight infeasible. This is evident even in countries subject to the GDPR.[154]

Thus, at least for now, state and federal actors cannot do it alone. As a result, academic researchers and investigative journalists have important roles in holding companies accountable and alerting consumers and agencies about known risks. The value of support is, of course, not news to regulators. For example, the FTC's settlement with Flo in 2021[155] stemmed from a *Wall Street Journal* investigation in 2019.[156]

As recently as March 2023, the FTC's Office of Technology has highlighted the value of assistance from researchers and journalists, particularly as it applies to pixel tracking.[157] Specifically, they identified five key areas for which researchers could help the FTC achieve its goals and protect consumers.[158] Those areas include industry conditions and competitive dynamics; consumer harms; business rationales; data processing, use, and monetization; and data retention and management.[159] We would add that this collaborative approach also helps broaden agency reach given the sheer size of the market for consumer health products like period and fertility tracking apps. This is not a perfect solution, but with more eyes on possible violators, the ability to meaningfully enforce existing rules against more actors expands.

---

154. *See* Koch et al., *supra* note 62.

155. *See In re Flo Health*, *supra* note 111.

156. Sam Schechner, *You Give Apps Sensitive Personal Information. Then They Tell Facebook,* WALL ST. J. (Feb. 22, 2019) https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636; *But see* What is the FTC Case https://help.flo.health/hc/en-us/articles/6498089874324-What-is-the-FTC-case- (asserting that the Wall Street Journal made inaccurate misrepresentations and denying any wrongdoing).

157. FTC Office of Technology, *Lurking beneath the surface: Hidden Impacts of Pixel Tracking,* (Mar. 16, 2023) https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking. Tracking pixels are small, hidden images (paired with HTML and JavaScript code) that developers embed in websites and emails that are capable collecting a wide variety of user data. *Id.* The primary uses for tracking pixels is to track consumer behavior (such as pageviews and ad interactions) and to target ads. *Id.*

158. *Id.*

159. *Id.*

IV. CONCLUSION

Despite representing relative and incremental improvements, the current patchwork of statutes, rules, and agencies has created a leaky regulatory sieve that period and fertility tracking apps pass through with relative ease. Even in jurisdictions with robust consumer protections or privacy laws, the highly sensitive nature of the data that period tracker apps collect means that users of those apps find themselves forced into particularly risky positions when the handlers of those data cannot be taken at their word. This risk is especially pronounced in light of various states' efforts to criminalize abortion[160] in the wake of the Supreme Court's *Dobbs* decision.[161] Nevertheless, menstrual data is just one (albeit highly important) component of the tapestry of data that data handlers profit from today. Outright lies and lies of omission that compromise consumer privacy occur across all technologies, and privacy harms matter even when they do not implicate something as high-profile as reproductive autonomy.[162]

Technology companies have a problem keeping promises. The inability to do something as simple as trust those who transact in our data to be honest and transparent in their claims has far-reaching implications for how we think about privacy moving forward. But lawmakers are doing little to tackle the problem of privacy lies head-on. There are no easy answers, and the collaborative approach we identify here is only a partial solution to a small piece of the problem of privacy. *Dobbs* threw these issues into stark relief, but we can use this moment as a catalyst to rethink and reshape the role of privacy in our everyday lives, helped along by researchers and journalists, who should make use of the power inherent in their knowledge. *Dobbs* and its fallout may represent a step backward, but we can also use it as an opportunity to step forward.

---

160. *See, e.g.,* TEX. HEALTH & SAFETY CODE § 170A.002, .004 (felony to "knowingly perform, induce, or attempt an abortion"); OKLA. STAT. TIT. 21 § 861 (felony to administer medicine or use an instrument to procure miscarriage unless to preserve life); Idaho Code § 18-606(2) (felony to induce or knowingly aid in the production of abortion in another, or for a woman to knowingly submit to an abortion, to solicit an abortion for herself or another, or to "terminate her own pregnancy otherwise than by a live birth").

161. *See generally* Dobbs, *supra* note 1.

162. *See generally* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U.L. REV. 793 (2022).