LEAK!
The Legal Consequences of Data Misuse in Menstruation-Tracking Apps

Tahsin M. Ahmed*

As patients become more sophisticated in managing their own health, they often turn to tracking apps to record and manage their health. Menstruation apps often track menstrual cycles, sexual activity, mood changes, and more. The Federal Trade Commission regulates these apps, but consistent with the common trend of law lagging behind technology, the extent of this regulation or lack thereof is not well understood. This Note investigates the legal consequences on user privacy, informed consent, and regulation when the data of menstruation-tracking apps is misused in the United States.

This research fills a gap in the literature by using the lens of international human rights to assess whether the data-sharing practices are sufficient to protect the right to privacy. Menstruation-tracking apps are not bound by the Health Insurance Portability and Accountability Act (HIPAA) because they are not healthcare providers. However, this Note argues that the function menstruation-tracking apps serve and the data they collect should compel these apps to comply with HIPAA to meet the human rights standard. This Note employs qualitative and quantitative analyses on past and present user agreements of the biggest menstruation-tracking app, Flo, as a case study.

DOI: https://doi.org/10.15779/Z38J38KJ7Z

* J.D. 2023, University of California, Berkeley, School of Law. The views and opinions expressed in this article are solely those of the author. They do not purport to reflect the views or opinions of any entities or individuals I affiliate with or represent. I would like to give a special thanks to Dr. Rohini Haar and Professor Eric Stover for their guidance and supervision throughout the writing and publishing process of this article. I would also like to thank Tam Ma, Cora Han, Marcy Wilder, and Rachel Nosowsky for their feedback and invaluable insight on this topic. Lastly, I thank the editors of the *California Law Review* for their tireless hours of hard work editing and providing feedback on this paper.

Introduction 1980
I. Issue 1982
II. Literature Review 1985
III. Methodology and Findings 1989
A. Qualitative Observations: Key Differences in Language 1989
B. Quantitative Observations: Reading Level Analyzer 1991
IV. Human Rights Standard for Informed Consent and Solutions to Protecting the Right to Privacy 1994
A. The Human Rights Standard for Informed Consent 1994
B. Proposed Regulatory and Corporate Policy Solutions 1997
Conclusion 1999

INTRODUCTION

Since the dawn of civilization, one fear has haunted almost half the human population: the risk of leaking during a menstrual cycle. However, the information age has brought a new concern that could potentially impact anyone with access to information technology such as the internet: the risk of a user's private data being leaked. What ties these issues to one another is the nigh-primordial[1] human need for privacy and the ways it can be compromised.

Although the meaning of privacy varies depending on the society and jurisdiction, the word encompasses concepts like the right to bodily integrity and freedom from invasive searches.[2] Privacy promotes values such as personal autonomy, respect, and human dignity.[3] Distinct but related concepts include confidentiality and security. Confidentiality is the nondisclosure of information collected in an intimate setting—patient-physician relationships being the most prominent example. Security is the technical and procedural measures that prevent private information from being leaked.[4] The value of privacy varies from person to person, but privacy benefits even those who find it unimportant by allowing them to control their social relationships.[5] A person's ability to control

1. *See Genesis* 3:7 (King James) ("And the eyes of [Adam and Eve] both were opened, and they knew that they were naked; and they sewed fig leaves together, and made themselves aprons."); *Al-Qur'an* 7:22 (Khattab trans.) ("And when [Adam and Eve] tasted of the tree, their nakedness was exposed to them, prompting them to cover themselves with leaves from Paradise.").

2. *The Value and Importance of Health Information Privacy*, *in* BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH 75, 76 (Sharyl J. Nass, Laura A. Levit & Lawrence O. Gostin eds., 2009) [hereinafter *Value and Importance*].

3. *Id.*

4. *Id.* at 76–77.

5. *Id.* at 77–78.

what others know about them is essential to preserving their dignity, which is a legally protected right under U.S. tort law.[6]

That privacy is a fundamental human right is well established in every major international and regional human rights instrument.[7] Article 12 of the Universal Declaration of Human Rights (UDHR) from 1948 states: "No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence."[8] Privacy is so central to human rights that it is the cornerstone upon which other rights are built, including the right to freedom of movement, thought, and association.[9] While a broad interpretation of privacy should apply to online transactions and digital data by that logic, in practice—as is often the case with law lagging behind technology—governments and service providers often fall short of meeting this standard.

Arguably, in no sector of life is privacy as essential as it is in health. The COVID-19 pandemic forced many people to turn to online resources to manage their health, such as by using telehealth services, conducting personal research into medical options, and seeking advice from the media.[10] Although technological advances have made patients more autonomous in managing their own health, such advances increase the risk of misinformation for commercial or political purposes.[11] Concerningly, not only does this trend erode patient health and their trust in the system, but it also obfuscates the commercial motivations of companies to push a certain product or to collect user data.

One way that smartphone users manage their health is by downloading health-tracking apps.[12] These apps rely on users inputting their health information such as their sleep cycle, mood, and fitness habits to analyze and visualize their health patterns.[13] Nearly 40 percent of American adults currently

---

6. *See, e.g.*, Raess v. Doescher, 883 N.E.2d 790, 798–99 (Ind. 2008) (finding that a doctor storming up to and yelling at his employee qualified as assault because the employee had an imminent apprehension of offensive contact). In this case, the doctor violated the employee's dignity by invading his personal space. *See also* Fisher v. Carrousel Motor Hotel, Inc., 424 S.W.2d 627, 630 (Tex. 1967) (finding that snatching a plate from a person constitutes battery because the defendant made offensive contact with the plaintiff and thereby violated the plaintiff's dignity).

7. *What Is Privacy*, PRIVACY INT'L (Oct. 23, 2017), https://privacyinternational.org/explainer/56/what-privacy [https://perma.cc/DP2Y-DFTY].

8. G.A. Res. 217 (III) A, art. 5, Universal Declaration of Human Rights (Dec. 10, 1948).

9. G.A. Res. 2200A (XXI), International Covenant on Civil and Political Rights (Mar. 23, 1976).

10. Tara Kirk Sell, *Meeting COVID-19 Misinformation and Disinformation Head-On*, JOHNS HOPKINS UNIV. BLOOMBERG SCH. OF PUB. HEALTH, https://publichealth.jhu.edu/meeting-covid-19-misinformation-and-disinformation-head-on [https://perma.cc/QYA2-2F4Y].

11. *Id.*

12. *See* U.S. DEP'T OF HEALTH & HUM. SERVS., EXAMINING OVERSIGHT OF THE PRIVACY & SECURITY OF HEALTH DATA COLLECTED BY ENTITIES NOT REGULATED BY HIPAA 9 (2016) [hereinafter EXAMINING OVERSIGHT], https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf [https://perma.cc/KD5E-96W6].

13. Mallory Creveling & Emily Goldman, *The 16 Best Health and Wellness Apps of 2021, According to Experts*, PREVENTION (Nov. 16, 2021), https://www.prevention.com/health/sleep-energy/g24736063/best-health-apps/ [https://perma.cc/7XUV-K7V9].

use a health-tracking app, and about one in three Americans have used digital health products in the past.[14] This Note specifically discusses menstruation-tracking apps, which are a subcategory of health-tracking apps that collect sensitive information on a user's menstrual cycle length, sexual activity, and urinary frequency.[15] Like any commercial app, these tracking apps collect user data, be it for marketing, development, or analytics purposes.[16] However, given the sensitive information that users input into these apps, the ethicality of companies using user data like this must be called into question.

This Note addresses three questions: (1) what are the legal consequences of data misuse in menstruation-tracking apps, (2) what should the standard be to preserve the human right to privacy, and (3) how can regulation change to reach that standard? First, I outline the issue and its regulatory landscape. Second, I discuss my methodology, which involves a literature review, interviews with professionals, and original research on the past and present terms of use and privacy policies of the largest menstruation-tracking app, Flo. Third, I discuss what changes in regulation and corporate practices would better protect people's data and thereby strengthen human rights.

I.
ISSUE

Menstruation-tracking apps are part of a broader trend in the tech industry called "femtech." Femtech is a category of "software, diagnostics, products, and services that use technology to support" people who menstruate.[17] This industry is highly lucrative: its market potential is forecasted to reach upwards of $60.1 billion by 2027.[18] Users are especially attracted to menstruation-tracking apps because many of these apps can purportedly assess when a user is ovulating based on their cycle and habits.[19] Many users treat these apps as birth control,

14. Anca Spanu, *More People Now Use Health Apps and Wearables, According to a Recent Survey*, HEALTHCARE WKLY. (Mar. 30, 2023), https://healthcareweekly.com/more-people-now-use-health-apps-and-wearables/ [https://perma.cc/KX4J-8NMZ]; *see* Justin McCarthy, *One in Five U.S. Adults Use Health Apps, Wearable Trackers*, GALLUP NEWS (Dec. 11, 2019), https://news.gallup.com/poll/269096/one-five-adults-health-apps-%20wearable-trackers.aspx [https://perma.cc/B65Y-B2WV] (discussing health-tracking app use in 2019).

15. Isobel Asher Hamilton, *Period Apps Are a Privacy Nightmare—Should You Still Use Them? An Expert Explains the Risks*, BUS. INSIDER (Jan. 28, 2021), https://www.businessinsider.com/period-apps-privacy-risks-ad-targeting-2021-1 [https://perma.cc/S2XA-US4M].

16. *Guess What? Facebook Still Tracks You on Android Apps (Even If You Don't Have a Facebook Account)*, PRIVACY INT'L (Mar. 5, 2019) [hereinafter *Guess What?*], https://privacyinternational.org/blog/2758/appdata-update [https://perma.cc/78RH-2G76].

17. Kathrin Folkendt, *So What Is Femtech, Anyways?!*, FEMTECH INSIDER (Sept. 5, 2019), https://femtechinsider.com/what-is-femtech/ [https://perma.cc/6RGU-635T].

18. Conor Stewart, *Worldwide Femtech Market Size 2019–2027*, STATISTA (Oct. 7, 2021), https://www.statista.com/statistics/1125599/femtech-market-size-worldwide/ [https://perma.cc/QQA3-BBVM].

19. *See, e.g.*, *Spot On Period Tracker*, PLANNED PARENTHOOD, https://www.plannedparenthood.org/spot-on-period-tracker [https://perma.cc/ZG9U-AMPP].

seeking to maximize or minimize their chance of getting pregnant by changing their sexual activity accordingly.[20]

A large problem regarding the privacy features of these apps is that they are produced by for-profit companies that are not healthcare providers. Accordingly, rules and guidelines promulgated by the Federal Trade Commission (FTC), not the Health Insurance Portability and Accountability Act (HIPAA), regulate these apps.[21] This means that protections that are normally applied to sensitive health data in the medical context do not automatically apply in the context of health- or menstruation-tracking apps.[22] Although the FTC has guidelines regarding data-sharing between apps, prior to 2019, many apps, including health apps, shared user data with web-hosting companies like Facebook and profiling companies like Braze or Amplitude.[23] These data transfers would often take place immediately once the user opened the app, before the user had a chance to indicate their consent or become aware that dissemination of this information was already occurring.[24]

In 2019, Privacy International released a series of reports analyzing a variety of apps and their data-sharing practices. The first report focused on companies sharing data through the Facebook Software Development Kit, which is a set of software development tools that help developers build apps.[25] The report found that the data was sent to Facebook with a unique identifier called a Google advertising ID, which made it easy for the company to link data and build a detailed profile on a user's interests, identities, and daily routines.[26] As a result of this report, most of the apps that Privacy International studied changed their data-sharing practices to require user consent first.[27] A similar report later came out that strictly examined menstruation-tracking apps, which similarly resulted in many of these apps overhauling their terms of use and privacy policies.[28]

---

20. Rasha Ali, *Do Period Tracker Apps Work as a Birth Control Replacement?*, USA TODAY (Aug. 8, 2019), https://www.usatoday.com/story/life/health-wellness/2019/08/08/can-period-tracker-apps-replace-condoms-and-pill-not-really/1888837001/ [https://perma.cc/Q2JS-XFWD].

21. Press Release, Fed. Trade Comm'n, FTC Warns Health Apps and Connected Device Companies to Comply with Health Breach Notification Rule (Sept. 15, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/09/ftc-warns-health-apps-connected-device-companies-comply-health-breach-notification-rule [https://perma.cc/6CRR-TRK3].

22. *Id.* I discuss FTC enforcement of regulations governing health apps later in this Note. *See infra* Part IV.B.

23. Hamilton, *supra* note 15.

24. *Investigating Apps Interactions with Facebook on Android*, PRIVACY INT'L (2019), https://privacyinternational.org/appdata [https://perma.cc/8C26-H3KZ].

25. *Id.*

26. *Id.*

27. *Id.*

28. *See No Body's Business but Mine: How Menstruation Apps Are Sharing Your Data*, PRIVACY INT'L (2019) [hereinafter *No Body's Business but Mine*], https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruations-apps-are-sharing-your-data [https://perma.cc/A38R-6B9V].

At the heart of this Note's human rights analysis is informed consent. Informed consent is the process of a person understanding and agreeing to their participation in an activity being used for other purposes, like research and medical testing.[29] However, app companies often have users consent to their terms with the tap of a single button labeled "Accept Terms & Conditions."[30] This method of gaining consent does more to legally protect the company collecting the data from future lawsuits and less to ensure that the user truly understands and consents to what the company is collecting.[31]

First, this Note investigates the legal consequences of data misuse in menstruation-tracking apps. To answer this question, I draw upon scholarly literature regarding data misuse of menstruation and health apps as well as why protecting user data matters. I examine the health impacts that these apps and their regulation have upon the user.

Second, this Note explores what legal standard would preserve the human right to privacy. My methodology involves analyzing the changes these companies made in response to the Privacy International recommendations; doing a side-by-side comparison of past and present terms of use and privacy agreements of Flo, the most popular menstruation-tracking app; and critically examining current methods of regulation.

Finally, this Note examines the regulatory framework governing menstruation-tracking apps. Companies are better equipped to protect user data than users themselves are. As compared to web browser cookies, it is much more cumbersome to block unwanted cookies on an app. As a result, few smartphone users opt out of third-party tracking while using apps that collect their most sensitive data.[32] Many apps that changed their agreements following Privacy International's exposé now include a clause in their agreements that stipulates they will deidentify data so the user cannot be singled out from the aggregate pool of consumer activity data. Once the company deidentifies that data, it no longer belongs to the user.[33] In this Note, I assess whether this policy change is a sufficient solution or whether menstrual health data is too sensitive to collect in even this limited capacity. I also argue that regulators should introduce a constitutional framework to protect user data and propose a hybrid approach to protecting sensitive health data so that HIPAA can apply to health apps.

29. *See* Christine Grady, Steven R. Cummings, Michael C. Rowbotham, Michael V. McConnell, Euan A. Ashley & Gagandeep Kang, *Informed Consent*, 376 NEW ENG. J. MED. 856, 856 (2017).

30. *See id.* at 857.

31. *Id.* at 858.

32. *Guess What?*, *supra* note 16.

33. Telephone Interview with Marcy Wilder, Former Deputy Gen. Couns., U.S. Dep't of Health & Hum. Servs. (Oct. 22, 2021).

II.
LITERATURE REVIEW

Although user privacy advocates have investigated many menstruation-tracking apps because of their suspicious data-sharing practices, very little is known about the specific uses of the data or the internal investigations that the app companies have conducted as recommended by accountability reports. To better understand the effects of data misuse by these apps, I turn to the literature.

Privacy International, an advocacy group dedicated to promoting more ethical technological privacy practices and educating users on their digital rights,[34] conducted its 2019 study on menstruation-tracking apps by comparing the privacy practices to the 2016 General Data Protection Regulation (GDPR).[35] The GDPR is the European Union's strictest privacy and security law.[36] Any company that processes the data of an EU citizen, even if the company is not located within the EU, must comply with the GDPR or risk a substantial fine.[37] The GDPR stipulates that a company must be transparent in its data processing practices, that it may collect no more data than is absolutely necessary to fulfill its stated goals, and that all consent must be "freely given, specific, informed and unambiguous."[38] Although compliance with the GDPR is only mandatory with respect to EU users and not those based in the United States, the law provides a helpful model for what reasonable informed consent practices look like.[39]

In its study of menstruation apps, Privacy International found that a majority of those apps that were also investigated for the Facebook data-sharing study had disabled the function that automatically shares user data with third-parties upon opening the app.[40] However, some of the less commonly used menstruation-tracking apps—such as the apps Maya and MIA, both of which had millions of users—still continued sharing the data with Facebook at that point.[41] According to a Maya spokesperson, "data" was kept safe within the app unless advertisers asked for it for targeted marketing purposes. However, the spokesperson did not clarify whether the specific data being shared involved health information like medical conditions or fertility.[42]

Using health information for marketing purposes poses potential risks to the user. As early as 2012, companies have used purchased data to determine

---

34. *Impact*, PRIVACY INT'L, https://privacyinternational.org/impact [https://perma.cc/YK3T-2WDW].

35. *No Body's Business but Mine*, *supra* note 28.

36. *See id.*

37. *What Is GDPR, the EU's New Data Protection Law?*, GDPR (2018), https://gdpr.eu/what-is-gdpr/ [https://perma.cc/6EGQ-NMD6].

38. *Id.*

39. *See* Tim Frick, *What Does GDPR Mean for US-Based Websites?*, MIGHTYBYTES (July 5, 2022), https://www.mightybytes.com/blog/what-does-gdpr-mean-for-us-based-websites/ [https://perma.cc/QA9S-3L39].

40. *No Body's Business but Mine*, *supra* note 28.

41. *Id.*

42. *Id.*

whether a user is pregnant to target the user with ads.[43] For example, Target assigned a "pregnancy score" to online shoppers by deducing what products pregnant people buy en masse. This eventually led to a lawsuit in which a father sued the company for mailing coupons for baby care items to their home before he knew his daughter was pregnant.[44] The potential dangers of a pregnancy being exposed without the consent of the expecting parent is well-documented, ranging from abuse by family and peers to poverty by disownment.[45] As such, private behaviors becoming public because of company misuse of data can have deleterious health impacts on the user. Stigma related to pregnancy status can result in depression and isolation.[46] Poverty resulting from disownment may cause physical, mental, and reputational harm.[47] Not only must users contend with companies knowing too much, but targeted advertising strategies may also hurt them in tangible ways.

The Privacy International report on menstruation apps found that the exact recipients of the data, the content and type of data shared, and whether companies anonymize the data are all unclear.[48] Despite this ambiguity, the report confirmed that the data of one demographic in particular is especially lucrative: pregnant women.[49] Whereas a data processing company might spend $0.10 for data on an average user, it could spend upwards of $1.50 (a whopping 1,400 percent increase) for the data of a pregnant person.[50]

In situations where profiling companies cannot access data that a user inputs, apps are still able to communicate sensitive health information without breaking their privacy agreements. For example, MIA's analysis function produces recommended articles based on the sexual activity a user inputs.[51] MIA then communicates to Facebook what articles were recommended to the user without disclosing information that the user entered into the app.[52] Although MIA cannot share with Facebook whether a user is likely pregnant based on user input, MIA enables Facebook to reach the logical conclusion that the user is pregnant by disclosing that MIA provided the user articles on pregnancy. The apparent loopholes and lack of transparency in company data-sharing practices

43. Kashmir Hill, *How Target Figured out a Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16, 2012), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=2d13e7366668 [https://perma.cc/K8MQ-S85H].

44. *Id.*

45. *See* Devi Akella & Melissa Jordan, *Impact of Social and Cultural Factors on Teenage Pregnancy*, 8 CTR. FOR HEALTH DISPARITIES RSCH. 3, 42 (2011); Alia Wong, *The Consequences of Teen Motherhood Can Last for Generations*, ATLANTIC (Mar. 11, 2019), https://www.theatlantic.com/family/archive/2019/03/bad-news-about-declining-teen-pregnancy-rates/584500/ [https://perma.cc/GU6K-HZRJ].

46. Wong, *supra* note 45.

47. *Id.*

48. *No Body's Business but Mine*, *supra* note 28.

49. *Id.*

50. *Id.*

51. *Id.*

52. *Id.*

make it difficult for users to understand how much of their inputted information actually stays protected within the app.

While the GDPR provides a solid framework for what companies should do to protect data and privacy, a lack of government enforcement of U.S. companies' practices undermines the goals of the policy. Thus far, it appears that menstruation apps that comply with GDPR standards are mainly doing so voluntarily or out of concern for public backlash.[53] While some companies comply with these standards better than others, the fact that menstruation apps are not bound by regulatory force to continue protecting user privacy may pose a problem if company leadership changes or financial incentives for compliance erode.[54]

The constitutional right to privacy may also play a role in informing how apps should treat privacy and data. Although no Supreme Court case addresses the issue of privacy practices with respect to private data head-on, some cases offer guidance on how much the right of privacy should be valued. The Supreme Court decision in *Bellotti v. Baird* established that the right to bodily autonomy and privacy is so strong that it overshadows a parent's right to receive parental notification before their child undergoes an abortion.[55] Moreover, in *Carpenter v. United States*, the Supreme Court found that some private data like cellphone location data is considered so sensitive that the government cannot access it without a warrant.[56] In fact, the Fourth Amendment's prohibition on invasions of privacy in places where individuals have a reasonable expectation of privacy played a key role in the outcome of *Carpenter*.[57]

That being said, a shortcoming of applying constitutional analyses to the issue of data privacy is that constitutional rights only apply against the government and not private persons or entities.[58] As such, businesses like menstruation-tracking apps do not have a constitutional obligation to protect user data. Ultimately, because app activity is not state action, turning to Fourth Amendment protections from illegal search and seizure (the seizure in question being apps collecting user data and transferring it elsewhere) may not be a reliable legal strategy to protect sensitive health information.[59] Despite this reality, past Supreme Court cases may make way for legal arguments for why

53. *See id.* With the greater media attention on data-sharing practices following the Privacy International report, companies likely fear losing users and revenue should another investigation take place.

54. *Id.* Clue is one example of an app that has practices more in line with the goals of the GDPR, as it allows users to use the app without an account and makes data deletion easier than on similar apps. *Id.*

55. *See* 443 U.S. 622, 651 (1979).

56. *See* 138 S. Ct. 2206, 2221 (2018).

57. *Id.*

58. *See* United States v. Jones, 565 U.S. 400, 406 (2012) ("[F]or most of our history the Fourth Amendment was understood to embody a particular concern for *government trespass* upon the areas . . . it enumerates." (emphasis added)).

59. *See id.* at 410–11.

private health information surrendered to menstruation-tracking apps should be treated with greater sensitivity than other types of data.

Although many of the legal consequences of data misuse by these apps are ambiguous, the literature provides insight into what may happen if that data is compromised. Targeted ads are one of the main results of data-sharing practices, and as explained earlier, using sensitive health data to produce ads can result in harmful health impacts on the user.[60] The data these apps collect contains massive amounts of personally identifiable information, much of which is sensitive or embarrassing. Thus, the intrinsic harm of this data being leaked is that private information may become known by others.[61] This implicates the importance of users being able to control their social relationships by regulating how much others know about them.[62]

Another harm users could face is economic harm. If medical information such as drug use, pregnancy status, or chronic conditions becomes available to insurers or the public, the user could potentially face discrimination, loss of insurance, or risk to their employment.[63] While users can fight discrimination in court, it is much more difficult for a user to hold companies accountable for the loss of opportunity. For example, if a prospective employer looks up the user on the internet and discovers sensitive health information that influences the employer to turn down the user, there is little the user can do to bring a case for discrimination.[64]

Lastly, data leaks may put users at risk of identity theft.[65] Medical information is highly prized to hackers because the personally identifiable information associated with it enables them to commit extortion or identity theft. Accordingly, medical records can sell for up to $1,000 on the web.[66]

These risks are all potential consequences of data leaks of sensitive information. However, due to the lack of transparency, it is unknown whether these leaks actually result from data misuse in menstruation apps. However, as long as these potential consequences exist, lawmakers should reconsider whether menstruation apps should be allowed to compromise data and risk exposing users to these harmful effects.

---

60. *No Body's Business but Mine*, *supra* note 28.

61. *Value and Importance*, *supra* note 2, at 93.

62. *See id.* at 78.

63. *See id.* at 80–81.

64. *See* Spokeo, Inc. v. Robins, 578 U.S. 330, 342 (2016) (finding that an injury in fact for intangible harm like employment discrimination can only be found if that injury is codified in statute).

65. *Value and Importance*, *supra* note 2, at 93.

66. Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH MAG. (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon [https://perma.cc/C955-8MSR].

III.
METHODOLOGY AND FINDINGS

I apply both qualitative and quantitative methods to understand informed consent in the terms of use and privacy policy of Flo, the most prominent menstruation-tracking app with upwards of two hundred million users.[67] The goal of this analysis is to determine whether the terms of service and privacy policy are easier to comprehend in the versions produced after the 2019 Privacy International report.

I use reading level and language as indicators of informed consent. Greater reader comprehension and simpler language make it more likely that a user understands what they are consenting to and thus yield greater privacy protection results. The qualitative approach looks at the agreement language and comments on what it includes or omits. This is a more subjective analysis, where I look at the actual wording, the complexity of the vocabulary, and the sentence structure of the agreements to determine which document is easier to understand. The quantitative approach uses a reading level analyzer tool to more objectively determine whether the agreements are comprehensible to a layperson. In this analysis, the lower a document's reading level, the easier it was to understand. [68]

To access the previous terms of use, I used the Wayback Machine, an online tool that preserves a page as it existed in a given time period. I located the 2021 version on Flo's current website. Both old and current versions of Flo's privacy policy are available on its website.

A. Qualitative Observations: Key Differences in Language

For this analysis, I observed differences in Flo's terms of use and privacy policy in the years before and after the Privacy International study. Specifically, I focused on the 2018 and 2020 terms of use and the 2016 and 2021 privacy policies.

To start, I made observations while reviewing the 2018 terms of use. The 2018 terms of use have a clause at the beginning that establishes that by consenting to the terms, the user consents to any subsequent changes that Flo makes to the terms without asking users to consent to the new terms.[69] I hypothesized that Flo would remove this clause because regulatory agencies forced genetic testing companies with similar clauses to alter their agreements. In 2018, 23andMe and Ancestry.com, upon which law enforcement relied to get genetic information in criminal cases, had to withhold client information from

67. Natasha Lomas, *Fertility Tracking App Flo Closes $50M Series B*, TECH CRUNCH (Sept. 9, 2021), https://techcrunch.com/2021/09/09/fertility-tracking-app-flo-closes-50m-series-b/ [https://perma.cc/CEF3-6W4V].

68. Michael Aldridge, *Writing and Designing Readable Patient Education Materials*, 31 NEPHROLOGY NURSING J. 373, 373 (2004).

69. *Flo Terms of Use*, FLO (July 16, 2018), https://flo.health/privacy-policy-archived/july-16-2018 [https://perma.cc/KJA2-J5ZY].

law enforcement for months while the companies waited for past clients to assent to the new consent agreements.[70] Those who did not consent did not have their data at risk of being surrendered to ICE.[71] This shift in the default—from consent by silence to companies seeking "express consent" before transferring user data—represents a trend towards greater preservation of user privacy.[72] In contrast, the 2018 Flo terms of use put the onus on the user to periodically look up the terms of use and be attuned to the changes therein.[73] Lastly, the 2018 terms of use stipulate that Flo may disclose identifying information about the user for purposes of legal action if the user violates the terms.[74]

By contrast, the 2020 terms provide more insight into the function of the app and what the user's rights are. The second clause clearly states that the company is not a licensed medical care provider and that its app is not designed to serve as birth control, a point of confusion in the past terms of use.[75] Additionally, the terms state that any changes to the terms will be accompanied by an email to the users and a request for express consent.[76] The terms establish that the app does not collect personal data from children under the age of thirteen.[77] However, notably, the new terms of use agreement does not mention how the app collects, uses, or shares data for users above the age of thirteen.[78] Even still, the new terms better inform users of the app's purpose and clarify that the app is not a substitute for a healthcare provider. These changes represent a step in the right direction towards empowering users to understand where their information goes and with whom it is shared.

To evaluate the privacy agreements, I compared the December 2016 privacy policy with the November 2021 privacy policy, the latest policy as of this study. The 2016 privacy policy has a similar clause to the 2018 terms of use indicating that continued use of the app means the user consents to the changes. However, unlike the 2018 terms of use clause, the 2016 privacy policy states that "material" changes to the privacy policy will be accompanied by an email informing users of the change.[79] As for data, the policy says that a user "may" choose to provide Flo access to personal information stored by third-party health

70. Thomas J. White, Former Chief Sci. Officer, Celera Corp., Forensic DNA Analysis in Criminal Investigations and Forensic Examinations Lecture at Berkeley Law (Nov. 2, 2021).

71. *Id.*

72. Mallory Locklear, *23andMe, Ancestry and Others Agree to Genetic Privacy Guidelines*, ENGADGET (July 31, 2018), https://www.engadget.com/2018-07-31-23andme-ancestry-genetic-privacy-guidelines.html [https://perma.cc/LR8S-HAPQ].

73. *Flo Terms of Use* (2018), *supra* note 69.

74. *Id.*

75. *Flo Terms of Use*, FLO (Feb. 5, 2020), https://web.archive.org/web/20200910193831/https://flo.health/terms-of-service [https://perma.cc/TUH6-HN7P].

76. *Id.*

77. *Id.*

78. *Id.*

79. *Flo Privacy Policy*, FLO (Nov. 15, 2016), https://flo.health/privacy-policy-archived/november-15-2016 [https://perma.cc/EV2U-VCJW].

sites.[80] This appears to be Flo's method of obtaining consent from the user to request data from other apps to import into Flo. The policy purports that it does not require the user to input personally identifiable information besides their name and email address. However, it also collects "recorded information regarding App usage" and location data without explaining why the app collects this information.[81] This harkens back to the GDPR guidelines that require apps collect only as much data as is necessary to fulfill the app's purpose, yet this clause violates that principle.

Even in 2016, Flo noted that it would share personal information in an aggregate and anonymous format along with data collected from other users.[82] This is notable because once information is deidentified, it no longer legally belongs to the user, and the company may do as it wills with it.[83]

Conversely, the 2021 privacy policy differs from the 2016 policy in its simplicity. In the 2021 policy, the sentences are shorter and written in active voice, which makes it easier for users to follow what the policy is communicating.[84] For example, the 2021 policy states "[y]ou can always withdraw your consent" in active voice that contrasts with the 2016 policy, which states "[i]t is up to you to review the applicable privacy policy of that system, as any information you have instructed us to share is subject to those policies." The 2021 policy expands the types of personal data the app collects and lists what kinds of information may be automatically collected.[85] While the actual data being collected has not changed much from 2016 to 2021, the 2021 policy promotes a clearer understanding of the information and rights a user surrenders when they consent to use the app.

A qualitative analysis of the terms of use and privacy policy reveals that the changes made after the 2019 report make the agreements easier to read and understand. Although Flo did not make any substantive changes to the policies themselves, the way Flo communicates its policies to the user marks a shift towards greater transparency and trends towards enabling users to make informed decisions about their data use.

B. Quantitative Observations: Reading Level Analyzer

I use reading level as a proxy for whether the average user can understand the agreement and thus give informed consent to its terms. Scholars have argued that patient materials should be written at an eighth-grade level maximum. But, to capture patients with functional illiteracy, these materials ideally should be

80. *Id.*
81. *Id.*
82. *Id.*
83. Telephone Interview with Wilder, *supra* note 33.
84. *Flo Privacy Policy*, FLO (Nov. 5, 2021), https://flo.health/privacy-policy-archived/nov-5-2021 [https://perma.cc/EL8F-4RWL].
85. *Id.*

written at a fifth-grade level.[86] Similarly, here, I argue that an app that collects and potentially shares health information should provide consent materials written at a fifth- to eighth-grade level.

To determine whether users are giving informed consent—whether they truly understand and agree to what they are reading—I ran each agreement through a reading level analyzing tool called the Automatic Readability Checker.[87] This tool averages the results of seven formulas used to determine the minimum reading level required to understand a passage. This method is inevitably imprecise because each equation relies on different indicators, such as sentence and word length, to determine whether the passage is comprehensible and disregards how frequently people of each educational range would encounter a given word. That being said, averaging the scores provides a general consensus on what the reading level would be.[88] Because the tool is limited to 3,000 words at a time, I ran the text of each agreement in batches of 3,000 words and averaged the results.

To interpret these results, one must focus on the reading level of the intended audience of the agreements. Terms of use and privacy policies are contracts, and the person agreeing to them is the audience. Because a significant portion of the population uses health-tracking apps that are similar to the menstruation-tracking app studied here,[89] I infer that the audience is composed mainly of laypeople who do not have a legal background and thus require a lower reading level to understand these agreements.[90] Although a subjective reading of these terms and agreements may lead one to believe that these documents are comprehensible to a layperson, the information being surrendered is so sensitive that it warrants a stricter standard of scrutiny, meaning a lower reading level. As of 2017, the average reading level in the United States is the eighth-grade level, so I base my findings on that standard.[91]

86. *See* Aldridge, *supra* note 68, at 373.

87. *Automatic Readability Checker*, READABILITY FORMULAS (2021), https://readabilityformulas.com/free-readability-formula-tests.php [https://perma.cc/SJX2-LUE9].

88. *Id.*

89. *See* Laura Ceci, *Number of Health and Fitness App Users in the United States from 2018 to 2022*, STATISTA (July 6, 2021), https://www.statista.com/statistics/1154994/number-us-fitness-health-app-users/ [https://perma.cc/F4BC-RG9T]; McCarthy, *supra* note 14.

90. McCarthy, *supra* note 14.

91. Lisa Marchand, *What Is Readability and Why Should Content Editors Care About It?*, CTR. FOR PLAIN LANGUAGE (Mar. 22, 2017), https://centerforplainlanguage.org/what-is-readability/ [https://perma.cc/P8ZM-XT4S].

Table 1: Reading Level Analyzer Results for Flo Terms of Use and Privacy Policies

Company Name	**Type**	**In-Effect Date**	**Reading Level**	**Inputted Word Length**
FLO	Terms of Use	2018	17 (College Graduate)	3014 + 1552 words long
FLO	Terms of Use	2020	13 (College Entry)	2916 + 1685 words long
FLO	Privacy	2016	14 (College Level)	2343 words long
FLO	Privacy	2021	13 (College Entry)	2957 + 1953 words long

Interestingly, the length of the terms of use both before and after the 2019 Privacy International report remained the same. However, the language had been drastically simplified. In fact, the major decrease in reading level required to comprehend the terms of use, from the college graduate level down to the college entry level, reflects this change. The college entry level is roughly equivalent to the high school graduate level. From 2018 to 2020, about 90 percent of the U.S. population were high school graduates, while only 35 percent of the population were college graduates. The reading level of these graduates likely maps onto the college entry level and college graduate level, respectively.[92] I find that a much larger population (a difference of 55 percent) would be able to understand the privacy policy in 2020 than in 2018.

The privacy policy in 2016 is relatively simple, whereas the privacy policy in 2021 is double the length of the 2016 agreement. Although the reading level appears to have gone down, the difference is likely negligible due to the imprecise method the algorithm uses. This seems consistent with the qualitative findings. For example, both agreements are relatively straightforward, and the 2021 policy is clearer and organized in a way that promotes user understanding of the policy.

Although the Flo agreements today are in more accessible language than they were before 2019, this progress still falls short of the goal of communicating at an eighth-grade level. In addition, with a terms of use agreement well over 3,500 words and a privacy agreement at almost 5,000 words, it is unlikely that a user can be reasonably expected to properly read through the terms before providing their consent.

92. *Educational Attainment Distribution in the United States from 1960 to 2021*, STATISTA (June 2, 2023), https://www.statista.com/statistics/184260/educational-attainment-in-the-us/ [https://perma.cc/G9Q4-LGTE].

IV.
HUMAN RIGHTS STANDARD FOR INFORMED CONSENT AND SOLUTIONS TO PROTECTING THE RIGHT TO PRIVACY

Overall, menstruation-tracking apps have made significant changes in the types of data they collect and with whom that data gets shared, both of which positively impact users.[93] Still, the United States lacks sufficient regulations to limit data use practices, and the EU does not rigorously enforce its existing regulations. As a result, nation states leave the door open for companies to renege on their commitment to preserve the privacy of sensitive health data with little recourse.[94] In this Part, I discuss the human rights standard for informed consent and the successes and failures of the current regulatory framework.

A. The Human Rights Standard for Informed Consent

In addition to the right to privacy, the human right to personal autonomy covers the right to make decisions about whether or not to share one's personal health information. These rights are encapsulated in the UDHR.[95] This means that people have a right to make decisions about their health and privacy, including the decision to disclose sensitive health information to a menstruation-tracking app. However, the decision to disclose this information does not negate the user's other human rights, such as the right to privacy. Central to the right to autonomy and privacy is informed consent.[96] As my research shows, medical research and corporate data-sharing practices require informed consent. Yet, the question that remains is where society should set the bar to determine whether the user has truly consented.

Considering that the user information that is stored in these apps is among the most sensitive of health data, the standard for informed consent should be very high. Menstrual health involves topics that are culturally stigmatized such as menstrual cycles, pregnancy status, sexual activity, and sexually transmitted diseases. As such, the social and psychological consequences of this data being leaked are of a delicate and potentially humiliating nature, elevating the need to adequately protect this information.

The consent agreements of menstruation apps are on the right track towards meeting this human rights standard of informed consent, but work still needs to be done to increase apps' transparency and decrease the amount of data they collect and share. As they exist today, the consent agreements of companies like

93. *No Body's Business but Mine*, *supra* note 28.
94. *Guess What?*, *supra* note 16.
95. *See generally* G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948).
96. *See* Grady et al., *supra* note 29, at 856.

Flo do not rise to the same level of reprehensibility as other, much larger companies.[97]

For context, to consent to a device company's product, a user can click "Agree" on a popup that asks if they agree to the terms and conditions.[98] However, embedded in every terms of use agreement within pages upon pages of complex legalese are provisions that stipulate that agreeing to one service is agreeing to the terms of many other products and services from that device company.[99] Though the way in which the information is communicated to the user in that case is far more pernicious than the way in which it is presented in the Flo agreements, the process of consent is the same: there is a notice of terms that the user can access, and if the user presses the button to indicate assent, then the onus is on the user for not reading the terms if anything goes awry.[100] However, my quantitative findings reveal a major flaw in this logic. Even if an average person were to read the terms of use of Flo, it is unlikely that they would comprehend what the terms stipulate.

The lack of transparency in the kinds of data that are collected and what that data is used for only further compounds this problem. For example, some newer smartphone devices ask a user if an app may track their activity.[101] If the user selects "Ask app not to track," the app can still send third parties a "digital fingerprint" of the user's device that includes technical information like its battery level and its IP address.[102] Such functions give users a false expectation of privacy and obfuscate how the app uses the data.[103] Therefore, the party that is best placed to ensure that user data is protected and not misused is the app company itself, not the user.

Furthermore, apps need to be held accountable for the impact they have on the health of their users. As discussed previously, data leaks of health information can lead to negative health impacts and social consequences, such as loss of employment opportunities.[104] Moreover, users trust menstruation-tracking apps to provide accurate information regarding their ovulation cycles in addition to reputable health articles and advice. When apps abuse that trust, the

97. *See generally* Jane Thomason, *Big Tech, Big Data and the New World of Digital Health*, 5 GLOB. HEALTH J. 165 (2021) (detailing massive health data collection and sharing practices of major tech giants).

98. *See* Curtis E.A. Karnow, *The Internet and Contract Formation*, 18 BERKELEY BUS. L.J. 135, 139 (2021).

99. *See id.* at 137.

100. *See id.* at 137–38.

101. Geoffrey A. Fowler & Tatum Hunter, *When You 'Ask App Not to Track,' Some iPhone Apps Keep Snooping Anyway*, WASH. POST (Sept. 23, 2021), https://www.washingtonpost.com/technology/2021/09/23/iphone-tracking/ [https://perma.cc/EK9F-NVEU].

102. *Id.*

103. *See id.*

104. *Value and Importance*, *supra* note 2, at 93.

user can be severely harmed.[105] For example, a common misconception among users is that menstruation-tracking apps can replace birth control because the apps can predict when the user is most fertile. Thus, it is critical that apps clarify that menstruation trackers are not replacements for contraceptives, like Flo did in its latest terms of use.[106] The risk of negative health impacts on users increases as technology becomes more sophisticated. For instance, some apps, like Natural Cycles, advertise themselves as birth control, yet users still become pregnant while using their services.[107] The Natural Cycles app has an extensive amount of influence over the user's behavior. Because of the imbalance of power between the app developers and the user, there needs to be an avenue for these companies to be held accountable if something goes wrong.

The interests being balanced here are (1) the user's human right to privacy, (2) the user's demand for a menstruation-tracking service, and (3) the company's profit motive to supply the menstruation-tracking service.[108] Of these interests, the human right to privacy outweighs the others, but that does not delegitimize the other two interests. Menstruation-tracking apps do not have to sell user data to web-hosting or profiling companies to profit from user activity. Services like Flo, Clue, and other menstruation-tracking apps have paid features that allow users to access a wide range of features while generating profit for the app.[109] Additionally, using menstruation-tracking apps could have a positive impact on a user's health. For example, the apps can send reminders to take medication, draw attention to irregularities in a user's menstrual cycle, and provide articles that promote the user's health and wellbeing.[110] However, because the user is in a vulnerable position by disclosing their personal sensitive information and trusting the apps to be accurate, the onus should be on the app to ensure that the user can rely on both the app's data security and health advice. Though companies may try to minimize the risk to users by anonymizing their data, they are still using data about a user's most intimate health experiences to make money regardless of whether the user contributes to the aggregate pool of health data. Health privacy is too important to human rights for these companies to make a profit from sharing data, but this does not preclude the companies from making money from more legitimate sources like subscriptions and other forms of user activity.

---

105. *Flo Period & Ovulation Tracker*, APPLE APP STORE (2021), https://apps.apple.com/us/app/flo-period-ovulation-tracker/id1038369065 [https://perma.cc/4R3S-9UJZ].

106. Ali, *supra* note 20.

107. Olivia Sudjic, *"I Felt Colossally Naive": The Backlash Against the Birth Control App*, GUARDIAN (July 21, 2018), https://www.theguardian.com/society/2018/jul/21/colossally-naive-backlash-birth-control-app [https://perma.cc/V3Z3-KM4W].

108. Karnow, *supra* note 98, at 126.

109. *See Flo Period & Ovulation Tracker*, *supra* note 105; *Clue Period & Cycle Tracker*, APPLE APP STORE (2021), https://apps.apple.com/us/app/clue-period-tracker-fertility/id657189652 [https://perma.cc/R2V7-UQCT].

110. *Clue Period & Cycle Tracker*, *supra* note 109.

B. Proposed Regulatory and Corporate Policy Solutions

Under the current regulatory framework, menstruation-tracking apps do not fall under the umbrella of healthcare providers that are bound by HIPAA, so the FTC regulates these apps instead. To address apps and services that specifically collect sensitive health data, the FTC released the Health Breach Notification Rule (the Rule) to hold companies that are not covered by HIPAA accountable for data breaches.[111] The Rule states that service providers that collect or use health data must notify consumers, the FTC, and occasionally even the media if there has been a security breach.[112] However, despite having the power to enforce the Rule, the FTC has been reluctant to do so.[113] This contrasts with providers who are bound by the HIPAA Security Rule, which the Centers for Medicare and Medicaid Services (CMS) enforces more strictly by partnering with other companies to audit covered entities.[114]

Moreover, companies like menstruation-tracking apps often misunderstand the requirements of the Rule, so they may be inadvertently failing to comply.[115] For instance, although menstruation-tracking apps are not covered by HIPAA, under the Rule, they are considered "health care providers" because they "furnish health care services."[116] Therefore, these apps are required to notify consumers and the FTC if any breach of health information occurs, including situations where a user's health information is shared with another company without the user's express consent.[117] Additionally, for apps like Flo that collect health data from other apps, this information is also covered under the Rule.[118] This is especially concerning because users expect apps to uphold their legal obligations and are unaware that those apps do not meet that standard.[119]

There are several ways that the FTC can increase accountability among app developers, such as by pursuing monetary penalties and injunctive relief. For example, in 2019, the D.C. Circuit Court affirmed the FTC's power under

111. FED. TRADE COMM'N, STATEMENT OF THE COMMISSION ON BREACHES BY HEALTH APPS AND OTHER CONNECTED DEVICES 1 (2021) [hereinafter FED. TRADE COMM'N, STATEMENT OF THE COMMISSION], https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf [https://perma.cc/3SAE-736K].

112. *Id.*

113. On February 1, 2023, the FTC announced a complaint against and proposed settlement agreement with GoodRx, a telehealth and prescription drug provider. *See* Stipulated Order for Permanent Injunction, Civil Penalty Judgment, and Other Relief at 1, United States v. GoodRx Holdings, Inc., No. 3:23-cv-460 (N.D. Cal. Feb. 1, 2023). Under the proposed order, GoodRx will pay a $1.5 million civil penalty for failing to report its unauthorized disclosure of consumer health data to third-party companies. *Id.* at 22. This is the first enforcement action that the FTC has brought under the Rule since the Rule's adoption in 2009.

114. *Id.*

115. *See Value and Importance*, *supra* note 2, at 98.

116. *Id.*

117. *See id.*

118. *See id.*

119. *See* EXAMINING OVERSIGHT, *supra* note 12, at 4.

Section 5 of the FTC Act to impose personal liability on company executives who are involved in deceptive practices. This decision paves a way for the FTC to apply penalties to the upper echelons of menstruation-tracking companies and the companies they share their data with.[120] Furthermore, in February 2023, the FTC brought its first enforcement action under the Rule.[121] The FTC entered a stipulated order with GoodRx, a telehealth and prescription drug provider, for failing to notify consumers and other parties of its unauthorized disclosures of consumers' individually identifiable health information.[122] The company agreed to pay a $1.5 million civil penalty for violating the Rule and may no longer share user health data for advertising purposes.[123] The FTC's employment of this novel injunction, in conjunction with the FTC's Statement of the Commission on Breaches by Health Apps and Other Connected Devices in which it reaffirmed that violators of the Rule face civil penalties, marks a shift towards greater regulation in the digital health space.[124] Whether the FTC will actively pursue these avenues to enforcement remains to be seen.

Another route to greater regulatory enforcement would be to create a constitutional argument. Earlier, I addressed the shortcomings of this approach, namely that the Constitution applies to the government and not necessarily to businesses.[125] However, one could liken technology companies to the government because of their massive surveillance capabilities, such as their ability to obtain user location data.[126] Drawing comparisons between the purpose of the Constitution and the role that these apps play in users' lives provides a way to introduce a constitutional framework into menstruation-tracking app regulation.

Another legal strategy that may promote greater user security and company accountability is to create an overlap between entities covered by HIPAA and the FTC. HIPAA provides advantages that menstruation-tracking app users can benefit from. HIPAA's Privacy, Security, and Breach Notification Rules set the national standard for privacy and security in the healthcare space.[127] The HIPAA

120. *See* Chris Jay Hoofnagle, Woodrow Hartzog & Daniel J. Solove, *The FTC Can Rise to the Privacy Challenge, but Not Without Help from Congress*, BROOKINGS INST. (Aug. 8, 2019), https://www.brookings.edu/articles/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress/ [https://perma.cc/WQZ9-6NSP].

121. Press Release, Fed. Trade Comm'n, FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising (Feb. 1, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising [https://perma.cc/74JP-6W3T].

122. *Id.*

123. SKADDEN, PRIVACY & CYBERSECURITY UPDATE: GOODRX AND EVOLVING DIGITAL HEALTH PRIVACY OVERSIGHT IN THE US 1–2 (2023), https://www.skadden.com/-/media/files/publications/2023/02/privacy-cybersecurity-update/privacy--cybersecurity-update-february-2023.pdf?rev=aad5fe7f062b4282a6badb560d02f910 [https://perma.cc/JK9K-26F2].

124. *See id.*; *see* FED. TRADE COMM'N, STATEMENT OF THE COMMISSION, *supra* note 111, at 2.

125. *See* United States v. Jones, 565 U.S. 400, 404–05 (2012).

126. *Guess What?*, *supra* note 16.

127. EXAMINING OVERSIGHT, *supra* note 12, at 11–19.

Security Rule applies to electronic medical records, but not health information stored in paper records.[128] This provision may open the door to the legal argument that menstruation-tracking apps operate like electronic medical records and thus need to be given a higher level of security.[129] Additionally, HIPAA applies to traditional healthcare entities but has expanded to include medical apps that transmit or store personal health information as well as clinics like Planned Parenthood.[130] Here, too, catalyzed by the COVID-19 pandemic, HIPAA may expand to digital health entities like menstruation apps as their use becomes more common.[131]

CONCLUSION

In conclusion, menstruation-tracking apps have the potential to positively impact user health, but their data-sharing practices do not meet a satisfactory human rights standard. First, there is little transparency: the types of data that are collected, how that data is used, and whom that data is sent to all remain unclear. In terms of informed consent, apps like Flo are making progress by changing their terms of use and privacy policies to be more accessible. However, the language is still vague and does not specify whether or how the companies use sensitive health data in their corporate practices. This issue raises the broader question of whether it is ethical at all to use health data for advertising or marketing purposes.

The solutions I propose include increasing FTC enforcement of existing policies, passing legislation that will create injuries in fact for users who are harmed by data breaches, and coercing companies through penalties to be more transparent in their use and misuse of user data. Ultimately, I find that the most effective avenue to protect user data would be to pursue civil penalties and injunctions through the FTC and extend HIPAA-like protections to menstruation-tracking app data.

At the forefront of any policy should be deference towards users' control over their privacy and information. App usage of consumer data is different from medical research in that the motivation behind data sharing is largely to generate profit instead of advancing science. However, this rationale is not sufficient to overcome the importance of preserving human rights. The risks to user health, such as the loss of dignity or employment opportunities, are too great to allow current data-collecting and data-sharing processes to continue as they are. The

128. *Value and Importance*, *supra* note 2, at 94, 97.

129. *See id.*

130. *See* Kirsten Peremore, *HIPPA and the FDA: Regulating Privacy in Medical Health Apps*, PAUBOX (June 13, 2023), https://www.paubox.com/blog/hipaa-and-the-fda-regulating-privacy-in-medical-health-apps#:~:text=Medical%20apps%20that%20handle%2C%20store,access%2C%20use%2C%20or%20disclosure. [https://perma.cc/X5P5-RX4W].

131. *See* EXAMINING OVERSIGHT, *supra* note 12, at 30–32.

responsibility must be put upon the companies, not the users, to protect this data because the companies have the resources and power to do so.

There are a number of research questions that, though outside of the scope of this Note, are worth exploring in future research. A critical next step includes investigating how changes in regulation may affect whether these services are viable as profitable companies. Putting too many restrictions on how data is collected, stored, and used may make operating a menstruation-tracking app too costly. This may have negative effects on the enormous user base that actively engages with these apps. Further research must be done on methods of holding apps accountable—are financial penalties sufficient, or does there need to be an injunction on certain app practices? Additionally, there is no evidence directly linking data breaches of menstruation-tracking apps to instances of identity theft or other severe consequences of data breaches. This begs the question of whether people have attempted to access users' personally identifiable information but were unable to due to apps' deidentifying practices, or whether data breaches of this sort are waiting to happen.