Period Tracking Apps' Data Privacy Concerns: A Case Study Analysis

Written and compiled by:
Anupama Bhatta

INTRODUCTION

In an era of increasing digitization, period tracking applications have emerged as essential tools for millions of women seeking to monitor their reproductive health. With over 200 million users worldwide, apps like Flo and Clue have transformed reproductive health tracking (Flo Health, 2023). These applications collect intimate data ranging from menstruation dates and cycle length to sexual activity, pregnancy intentions, and physical symptoms—information that users entrust to these platforms with the expectation of privacy and confidentiality.

However, beneath the convenience of these digital health tools lies a complex ethical dilemma centered on data privacy. Despite promises of confidentiality, many period tracking applications have been found to share users' sensitive reproductive health information with third parties, including advertising platforms, analytics services, and data brokers (Federal Trade Commission, 2021). This practice creates significant ethical tensions between users' privacy rights and corporate data monetization strategies, particularly in the post-Roe v. Wade landscape where reproductive health data has acquired new legal significance and potential risks.

When the Wall Street Journal exposed that Flo had shared sensitive user data with Facebook and Google in 2019, hundreds of users reported feeling "outraged," "violated," and "appalled" (FTC, 2021, p. 6).

Can users meaningfully consent to data practices they don't fully understand, and should corporations prioritize user privacy over profit motives when handling sensitive health information?

This analysis aims to identify values and approaches that information professionals can marshal to address these ethical challenges and position themselves as trusted protectors of sensitive health data in a digital ecosystem that increasingly blurs the boundaries between healthcare, technology, and commerce.

CASE BACKGROUND

Period tracking applications represent a rapidly growing sector of health technology, with the market expanding dramatically since 2016. Apps like Flo and Clue dominate this landscape, with tens of millions of active users globally (Torchinsky, 2022). These apps primarily operate through freemium models while relying heavily on data collection for revenue (Hammond & Burdon, 2024).

Users regularly input highly sensitive information, including sexual activity, physical symptoms, medication use, contraception methods, and pregnancy intentions (Burke, 2024). This comprehensive health tracking creates detailed profiles of users' reproductive lives and overall wellbeing.

The privacy practices of period tracking apps came under scrutiny in 2019 when the Wall Street Journal revealed that Flo Health had been sharing sensitive user data with Facebook, Google, and analytics firms despite explicit privacy promises (FTC, 2021). This led to formal FTC complaints and a settlement requiring Flo to obtain explicit user consent before sharing health data (Federal Trade Commission, 2021). Subsequent independent research by privacy advocacy organizations identified widespread privacy and security issues across the reproductive health app ecosystem (Mozilla, 2022).

These concerns intensified after the 2022 Supreme Court decision overturning Roe v. Wade, which catalyzed significant user migration between period tracking apps (Perez, 2022). With abortion access now criminalized in multiple states, period tracking data could potentially be used in law enforcement investigations, transforming what was once a consumer privacy issue into a matter with significant legal and safety implications (Torchinsky, 2022).

This landscape reflects the evolution of period tracking technology from simple calendar tools to sophisticated data collection systems operating at the intersection of healthcare, technology, and law.

ETHICAL DILEMMA

At the heart of the period tracking app controversy lies a fundamental ethical dilemma: the tension between users' right to privacy for their intimate health data and the commercial interests driving app developers to collect, share, and monetize this information.

The primary ethical tension stems from the nature of the data being collected. Menstrual and reproductive health information is among the most sensitive personal data individuals can share, touching on intimate aspects of bodily autonomy, sexuality, and reproductive choices. As Roberts notes, "If ever there was a concrete example of the harms [of data sharing], boy do we have one" (Roberts, 2022). This sensitivity is heightened by the fact that such data can potentially reveal pregnancy status, fertility attempts, or pregnancy termination—information that now carries legal risks in multiple jurisdictions.

The ethical dilemma is compounded by issues of informed consent. Despite privacy policies that technically disclose data sharing practices, these documents are typically written in complex legal language and buried within terms of service. Mozilla's research found that many apps employ "data first, then consent" models where information collection begins before meaningful consent is obtained (Mozilla, 2022). This raises serious questions about whether users can genuinely consent to data practices they don't comprehend or have realistic alternatives to avoid.

Furthermore, the power imbalance between individual users and technology companies amplifies ethical concerns. Users seeking essential health management tools face a "privacy paradox"—needing the functionality of period tracking but being required to surrender intimate data to obtain it (Hammond & Burdon, 2024). When Flo's practices were exposed, users expressed feeling "victimized" and "violated" by this betrayal of trust, highlighting the emotional and psychological dimensions of the ethical breach (FTC, 2021, p. 6).

What transforms this from a mere policy disagreement into a profound ethical dilemma is that both sides have legitimate claims. Users have reasonable expectations of privacy and bodily autonomy, while companies face market pressures to generate revenue and develop superior products through data collection. The clash between these values—privacy versus utility, individual rights versus business sustainability—creates a dilemma where no solution fully satisfies all moral considerations without significant compromise of fundamental principles.

PROFESSIONAL AND SOCIETAL ISSUES

The ethical dilemmas surrounding period tracking apps extend beyond individual privacy concerns to broader professional and societal implications that affect multiple domains of information ethics. Information professionals face particular challenges in this landscape as they navigate competing obligations to users, organizations, and society at large.

From a professional ethics perspective, information professionals involved in the development, deployment, and governance of health tracking technologies face significant responsibilities. They must balance their duty to facilitate technological innovation with obligations to protect sensitive user data. As Coppieters and Levêque (2013) note, "Ethics, legal frameworks and privacy are often the subject of much confusion in discussions among healthcare professionals" (p. 1). This confusion is particularly pronounced in the femtech sector, where traditional health information governance frameworks often fail to address the unique challenges posed by consumer-facing reproductive health technologies operating outside medical contexts (McCallum, 2022).

The societal implications are equally profound. Period tracking apps present a clear healthcare accessibility benefit, offering free or low-cost reproductive health tracking to populations who might otherwise lack access to such tools. Yet this accessibility comes with significant privacy trade-offs that disproportionately affect vulnerable populations. As Boyd argued in Mozilla's research, "Apps and devices that millions of people trust have the potential to be used to prosecute people seeking abortions" (Mozilla, 2022). This creates a disturbing dynamic where those most in need of reproductive healthcare tools face the greatest privacy risks in using them.

The global perspective further complicates these issues. European users benefit from GDPR protections that American users lack, creating geographic disparities in privacy protections (Clue, 2025). This inconsistency raises questions about equitable protection of intimate data across borders and jurisdictions. For example, Clue's status as a German company operating under GDPR offers certain protections that American companies cannot match under current U.S. privacy regulations (Torchinsky, 2022).

Perhaps most concerning is the emerging surveillance architecture that period tracking apps contribute to. Unlike previous eras where reproductive healthcare was largely private, today's digital ecosystem creates extensive documentation of reproductive health choices that can be accessed by corporations, governments, and potentially hostile actors. As Galperin noted, "Since the advent of Roe v. Wade, we've built an entire surveillance state in which every person is carrying a tracking device in their pocket" (Roberts, 2022). This fundamental shift transforms reproductive healthcare from a private medical matter to a potentially surveilled activity with significant social, legal, and personal ramifications.

STAKEHOLDERS AND POSITIONS

The period tracking app ecosystem involves multiple stakeholders with diverse and often conflicting interests in how reproductive health data is handled.

App developers and companies present themselves as champions of women's health empowerment while operating business models that often rely on monetizing user data. When privacy breaches were exposed, companies like Flo and Clue rapidly shifted positions—introducing "Anonymous Mode" features and emphasizing GDPR compliance as competitive advantages (Flo Health, 2023; Clue, 2025).

Users and privacy advocates form a crucial stakeholder group with distinctly different priorities. Research indicates users feel "powerless and uninformed about risk mitigation practices" despite significant concerns about data sharing (Cao et al., 2024). Privacy advocacy organizations like Mozilla Foundation have become increasingly vocal, conducting independent evaluations of app privacy practices and pushing for greater transparency. Their investigation found 18 of 25 reproductive health apps failed to meet basic privacy standards (Mozilla, 2022).

Data brokers and third-party entities process reproductive health data as part of broader advertising ecosystems with minimal transparency regarding downstream uses. As detailed in the consolidated class action complaint against Flo, third parties receive "vital" health data for "marketing and data analytics purposes" (Frasco v. Flo Health Inc., 2021).

Regulatory bodies, particularly the Federal Trade Commission, established that misrepresenting health data sharing practices constitutes a deceptive trade practice requiring remediation (Federal Trade Commission, 2021). However, current enforcement mechanisms remain insufficient to address the scale of the problem.

Healthcare professionals encounter patients who use period tracking apps as supplementary health tools yet have little input into their design or governance.

ETHICAL ANALYSIS

The ethical implications of period tracking apps' data practices can be examined through several philosophical frameworks that provide insight into the complex value conflicts at play. By applying consequentialist, deontological, and care ethics perspectives, we can better understand the moral dimensions of this technological dilemma.

From a consequentialist viewpoint, the ethical assessment hinges on balancing beneficial and harmful outcomes. Period tracking apps provide significant health benefits by empowering users with insights about their reproductive cycles, potentially improving healthcare access for underserved populations (McCallum, 2022). However, these benefits must be weighed against the potential harms of privacy violations, including emotional distress, discrimination, and legal risks in jurisdictions where reproductive choices are criminalized.

The Mozilla Foundation's research demonstrates that the "data buffet practice" of excessive collection creates disproportionate risks compared to the functionality provided (Mozilla, 2022).

Deontological ethics, focusing on duties and rights, offers a different perspective. This framework emphasizes users' fundamental right to privacy and bodily autonomy as inviolable principles. As articulated in ethical frameworks for health data, "privacy as a fundamental right" should be prioritized over commercial interests (Xafis et al., 2019). The duty of transparency is particularly relevant—many apps fail this obligation by employing what researchers call "data first, then consent" models that collect information before obtaining meaningful permission (Mozilla, 2022). This pattern violates the ethical principle that "consent should be obtained freely, without any coercion" (Atlan, 2024).

Care ethics, which emphasizes relationships and contextual responsibilities, highlights the intimate nature of reproductive health information and the special duty of care required when handling such data. This approach recognizes the relational context of period tracking—users share deeply personal information based on trust, creating obligations beyond mere contractual terms. As the Ethics Framework for Big Data in Health explains, "Information relating to health derives its sensitivity from the prospective harm to individual welfare or dignity" (Xafis et al., 2019).

The tension between these ethical frameworks reveals competing values that cannot be fully reconciled in current app designs. While consequentialism might justify some data collection to improve services, deontological and care perspectives emphasize how current practices undermine fundamental rights and relational trust. This analysis suggests an ethical approach that prioritizes transparency, meaningful consent, and data minimization—collecting only what is necessary for functionality rather than what is profitable for businesses (Roberts, 2022). The ethical ideal would be apps that provide health benefits while respecting user autonomy and privacy as non-negotiable values, rather than treating them as commodities to be traded for services.

VALUES AND APPROACHES

Information professionals working in technology, healthcare, and data governance can draw upon several key professional values and practical approaches to address the ethical challenges posed by period tracking applications and similar health technologies.

The foundation of ethical practice in this domain must be built on respect for user autonomy—recognizing individuals' rights to control their health information as an extension of their bodily autonomy. This principle is central to ethical frameworks for health data management, which emphasize that "data concerning health must serve the individual" (Clue, 2025). For information professionals, this means championing privacy by design principles that integrate privacy protections into technology development from conception rather than adding them as afterthoughts (Torchinsky, 2022).

Data minimization represents another crucial value for ethical information management. The practice of collecting only what is necessary for functionality—rather than what might be commercially desirable—stands in contrast to the "all you can collect and share data buffet practice" currently prevalent in the industry (Mozilla, 2022). This approach is supported by both ethical frameworks for health data and emerging regulatory standards, which increasingly recognize that excess data collection creates unnecessary privacy risks (Xafis et al., 2019).

Transparency and informed consent must guide interactions with users. As Boyd argues, "Companies collecting personal and sensitive health information need to be extra diligent" in clearly communicating data practices (Mozilla, 2022). Information professionals should advocate for plain-language privacy policies, contextual consent processes, and ongoing education about data risks—moving beyond the legal fiction that users meaningfully consent to practices buried in lengthy terms of service documents.

Tools for ethical decision-making in this space include structured privacy impact assessments that systematically evaluate how technologies affect user privacy. Health and privacy researchers advocate applying the "hexa-dimension framework" for data ethics, which evaluates technologies across legal validity, social desirability, ecological sustainability, ethical acceptability, technical effectiveness, and financial viability (Lee, 2016). This multidimensional approach prevents technical or financial considerations from overshadowing ethical concerns during technology development.

Professional codes of ethics in information science and data management provide additional guidance. These codes typically emphasize obligations to protect confidentiality, obtain informed consent, maintain data security, and prioritize user interests when conflicts arise. The ethics framework developed by the Science, Health and Policy-relevant Ethics in Singapore (SHAPES) Initiative offers specific guidance for health data, identifying procedural values including transparency, engagement, reflexivity, and accountability as essential for ethical data governance (Xafis et al., 2019).

By integrating these values and approaches, information professionals can help transform the period tracking app landscape from one dominated by exploitative data practices to one that centers user privacy while still delivering innovative health services. This requires moving beyond technical compliance with regulations to embrace substantive ethical commitments that prioritize user autonomy and data protection as fundamental professional responsibilities.

INFORMATION PROFESSIONALS AS TRUSTED ACTORS

Information professionals occupy a uniquely important position to address the ethical challenges presented by period tracking apps. As mediators between users, developers, and regulatory frameworks, these professionals can establish themselves as trusted actors who prioritize both technological advancement and fundamental privacy rights.

The role of information professionals extends beyond technical implementation to include advocacy for ethical data practices. As Hammond & Burdon (2024) argue, period tracking apps currently impose "control-based harms and intimate harms" that require moving beyond traditional information privacy models. Information professionals must advocate for holistic privacy protections that recognize the deeply intimate nature of reproductive health data, rather than treating it as generic information assets. This means actively challenging the notion that extensive data collection is necessary for functionality and instead promoting privacy-preserving alternatives (Roberts, 2022).

Building trust requires demonstrating consistent commitment to privacy protection. According to Mozilla's research, only one period tracking app (Euki) earned their "Best Of" privacy certification, highlighting the significant opportunity for information professionals to differentiate themselves through robust privacy practices (Mozilla, 2022). Trust-building strategies should include transparent data policies written in accessible language, user-friendly privacy controls, and proactive disclosure of all data sharing relationships.

Professional advocacy can take multiple forms, including participating in policy development at organizational and governmental levels. Information professionals should advocate for special classification of reproductive health data under privacy regulations, similar to protections afforded to other sensitive health information (Coppieters & Levêque, 2013). Through engagement with professional associations and regulatory agencies, information professionals can help shape emerging privacy frameworks to better address the unique challenges of reproductive health data.

The educational responsibilities of information professionals are equally crucial. Digital literacy programs should help users understand the privacy implications of period tracking apps and evaluate risk factors when choosing between services. As Torchinsky advises, users in states with restrictive reproductive health laws should exercise particular caution with digital tracking tools (Torchinsky, 2022). Information professionals can develop educational resources that explain complex privacy concepts in accessible terms, empowering users to make informed decisions about their reproductive health data.

RECOMMENDATIONS

To address the ethical challenges surrounding period tracking apps, I recommend a multi-faceted approach balancing innovation with privacy protection. App developers should implement privacy by design principles, incorporating data protection from the earliest stages of development (Mozilla, 2022). This includes adopting local storage options where data remains on users' devices instead of company servers (Roberts, 2022).

Policy reforms should establish reproductive health data as a special category requiring enhanced protections. Legislators should consider adapting existing health privacy frameworks to cover consumer health apps, closing the regulatory gap that currently leaves reproductive health data vulnerable (Coppieters & Levêque, 2013). The FTC's application of the Health Breach Notification Rule represents a positive step, but more comprehensive protections are needed (Federal Trade Commission, 2021).

User education initiatives must be prioritized to empower informed decision-making. Digital literacy programs should teach users to evaluate app privacy practices, understand terms of service implications, and implement available privacy protections. As research shows users feel "powerless and uninformed about risk mitigation practices," closing this knowledge gap is essential (Cao et al., 2024).

Technical safeguards should be standardized across the industry, including encryption, minimized retention periods, and anonymization techniques. The contrast between apps with weak security and those with meaningful protection highlights the need for minimum security standards (Mozilla, 2022).

Most importantly, the femtech industry must shift from data exploitation models toward privacy-centered approaches that prioritize user welfare. As Clue's co-CEOs assert, reproductive health data "must serve the individual" rather than corporate interests (Tsang & Walter, 2022). This requires reimagining business models that can sustain development without compromising user privacy.

CONCLUSION

The case of period tracking apps illuminates the profound ethical challenges that emerge when intimate health data intersects with commercial technology. The fundamental tension between users' privacy rights and corporate data practices creates complex dilemmas that require substantive ethical frameworks recognizing the special sensitivity of reproductive health information.

This analysis has demonstrated that meaningful protection of reproductive health data demands moving beyond conventional privacy models toward approaches that acknowledge the intimate nature of this information and its connection to bodily autonomy. As Hammond & Burdon (2024) argue, we need a privacy framework that is "relational, context-dependent and acknowledges the connection between intimacy and privacy."

Information professionals have a crucial opportunity to position themselves as ethical guardians—advocating for robust privacy protections, developing privacy-enhancing technologies, and empowering users through education. By centering ethical values of autonomy, care, and justice in the development of reproductive health technologies, information professionals can help transform period tracking apps from potential surveillance tools into trustworthy resources.

The stakes extend beyond individual privacy to fundamental questions about reproductive autonomy in a digital age. As reproductive rights face increasing legal challenges, protecting the privacy of reproductive health data becomes not merely a technical concern but a matter of ensuring that digital technologies serve as tools of empowerment rather than instruments of control.

REFERENCES

Atlan. (2024, December 7). Data ethics in 2025: Principles, frameworks & key challenges. https://atlan.com/data-ethics-101/

Burke, S. (2018, May 11). Your menstrual app is probably selling data about your body. VICE. https://www.vice.com/en/article/menstrual-app-period-tracker-data-cyber-security/

Cao, J., Laabadli, H., Mathis, C., Stern, R., & Emami-Naeini, P. (2024, May 11-16). "I deleted it after the overturn of Roe v. Wade": Understanding women's privacy concerns toward period-tracking apps in the post Roe v. Wade era. CHI '24, Honolulu, HI, USA. https://doi.org/10.1145/3613904.3642042

Clue. (2025, January 19). Clue privacy policy. https://helloclue.com/privacy

Coppieters, Y., & Levêque, A. (2013). Ethics, privacy and the legal framework governing medical data: Opportunities or threats for biomedical and public health research? Archives of Public Health, 71, 15. https://doi.org/10.1186/0778-7367-71-15

Federal Trade Commission. (2021). Complaint in the matter of Flo Health, Inc. (Docket No. C-4747).

Federal Trade Commission. (2021, June 22). FTC finalizes order with Flo Health, a fertility-tracking app that shared sensitive health data with Facebook, Google, and others. https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google

Flo Health. (2023, November 2). Flo Health's "Anonymous Mode" feature recognized as one of TIME's List of Best Inventions 2023. https://flo.health/newsroom/time-best-inventions-2023

Frasco v. Flo Health, Inc., Case No. 3:21-cv-00757-JD (N.D. Cal. 2021).

Hammond, E., & Burdon, M. (2024). Intimate harms and menstrual cycle tracking apps. Computer Law & Security Review. https://doi.org/10.1016/j.clsr.2024.106038

Lee, W. W., Zankl, W., & Chang, H. (2016, December 24). An ethical approach to data privacy protection. ISACA Journal. https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/an-ethical-approach-to-data-privacy-protection

McCallum, S. (2022, May 6). Period tracking apps warning over Roe v Wade case in US. BBC News. https://www.bbc.com/news/articles/cmj6j3d8xjjo

Mozilla. (2022, August 17). In post Roe v. Wade era, Mozilla labels 18 of 25 popular period and pregnancy tracking tech with *Privacy Not Included warning. https://foundation.mozilla.org/en/blog/in-post-roe-v-wade-era-mozilla-labels-18-of-25-popular-period-and-pregnancy-tracking-tech-with-privacy-not-included-warning/

Perez, S. (2022, June 27). Consumers swap period tracking apps in search of increased privacy following Roe v. Wade ruling. TechCrunch. https://techcrunch.com/2022/06/27/consumers-swap-period-tracking-apps-in-search-of-increased-privacy-following-roe-v-wade-ruling/

Roberts, C. (2022, May 25). These period tracker apps say they put privacy first. Here's what we found. Consumer Reports. https://www.consumerreports.org/health/health-privacy/period-tracker-apps-privacy-a2278134145/

Torchinsky, R. (2022, June 24). How period tracking apps and data privacy fit into a post-Roe v. Wade climate. NPR. https://www.npr.org/2022/05/10/1097482967/roe-v-wade-supreme-court-abortion-period-apps

Tsang, A., & Walter, C. (2022, July 26). Data is power, and responsibility: What we believe as Clue's co-CEOs. Clue. https://helloclue.com/articles/about-clue/data-is-power-and-responsibility-what-we-believe-as-clue-s-co-ceos

Xafis, V., Schaefer, G. O., Labude, M. K., Brassington, I., Ballantyne, A., Lim, H. Y., Lipworth, W., Lysaght, T., Stewart, C., Sun, S., Laurie, G. T., & Tai, E. S. (2019). An ethics framework for big data in health and research. Asian Bioethics Review, 11(3), 227-254. https://doi.org/10.1007/s41649-019-00099-x