Contraception xxx (xxxx) xxx

Contents lists available at ScienceDirect

Contraception

journal homepage: www.elsevier.com/locate/contraception

Experiential case study audit of three popular period trackers using General Data Protection Regulation (GDPR) and intimate privacy assessment criteria☆,☆☆

Pamela M. White [a,*], Niamh Fuller [b], Allison M. Holmes [c], Virginia Franqueira [d]

[a] Kent Law School, University of Kent, Canterbury, Kent, United Kingdom
[b] Technology Linklaters LLP, London, United Kingdom
[c] Birmingham Law School, University of Birmingham, Edgbaston, Birmingham, United Kingdom
[d] School of Computing, University of Kent, Canterbury, Kent, United Kingdom

ARTICLE INFO

Article history:
Received 11 September 2024
Received in revised form 18 September 2025
Accepted 19 September 2025

Keywords:
Consent
Data harms
Femtech
General Data Protection Regulation
Intimate privacy
Period trackers

ABSTRACT

Objectives: Period tracker downloads worldwide continue to increase year over year even though users are exposed to intimate data surveillance, unconsented third-party data sharing, and unauthorized commercial use of their reproductive information. This paper argues that data protection measures such as Europe's General Data Protection Regulation, considered the gold standard for personal privacy protection, could be bolstered if an intimate privacy design code was applied.

Study design: As no code, such as the United Kingdom Information Commissioner's Children's Code, exists for reducing data protection risks associated with online processing of sensitive reproductive information, we developed 15 measures operationalizing the concept of intimate privacy. Risk assessments based on intimate privacy criteria were compared to General Data Protection Regulation requirements in our 2023 United Kingdom–based pilot study auditing three popular period trackers, Flo, Clue, and Eve.

Results: When our intimate privacy criteria were applied, we identified tracker data protection weaknesses and privacy elements falling outside of existing General Data Protection Regulation requirements. Particularly worrisome was the lack of dynamic consent for data sharing, no built-in surveillance detection measures, and few user–determined data retention and deletion processes. Processing and storage of United Kingdom Flo and Eve users' data in the United States raises significant intimate privacy protection concerns, especially as legal implications of such data transfers were not well explained to users. Privacy policies were complex, requiring college education.

Conclusions: Incorporating intimate privacy-by-design would provide Femtech device users enhanced protection for their sensitive, private intimate data.

1. Introduction

In the wake of the 2022 *Dobbs v Jackson Women's Healthcare Institution* decision, American period tracker users were advised to delete their data and warned to refrain from commenting about their fertility status when using social media [1]. While studies demonstrate that period trackers expose users to privacy harms, including surveillance [2], unconsented third-party data sharing [3], and unauthorized commercial use of personal health and fertility data [4], tracker downloads worldwide continue to increase year over year [5].

Kelly and Habib [6] in their review of tracker data harms observe that Europe's General Data Protection Regulation's (GDPR) mandated privacy policies and explicit consent for health information processing offer safeguards not found in United States (US) law. Yet research reveals that GDPR required privacy policies are complex, rarely read, and poorly understood by consumers [7]. Solove contends that the GDPR's explicit, informed consent requirement does not prevent data subjects from engaging in a murky "all-or-nothing" consenting process [8]. Moreover, Citron [9] argues that the duty to protect intimate privacy rests with lawmakers and manufacturers,

☆ Conflicts of interest: Pamela M. White, Naimh Fuller, Allison M. Holmes, and Virginia Franqueira declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

☆☆ Funding: Niamh Fuller reports that financial support was provided by the University of Kent. This work was supported by the University of Kent, School of Computing, ICSS Seedcorn Grant 2023.

* Corresponding author.
E-mail address: p.white-229@kent.ac.uk (P. White).

https://doi.org/10.1016/j.contraception.2025.111235

Please cite this article as: P.M. White, N. Fuller, A.M. Holmes et al., Experiential case study audit of three popular period trackers using General Data Protection Regulation (GDPR) and intimate privacy assessment criteria, Contraception, https://doi.org/10.1016/j.contraception.2025.111235

whereas the onus to achieve data protection often resides with poorly informed and ill-equipped users.

In response to privacy concerns raised by United Kingdom (UK) period tracker users and researchers highlighting poor data security [10], problematic data accuracy [11], and troubling consenting practices [12] the UK Information Commissioner's Office (ICO), the organization mandated to enforce the UK GDPR, held public consultations and commissioned a user survey. Their 2023 consultation and survey report [13] confirmed readability problems with privacy policies and documented user lack of trust in tracker security features. Unlike the US Health Insurance Portability and Accountability Act (HIPAA), which excludes tracker data from its health data protection remit, the scope of the GDPR Art. 9 sensitive health information protections is significantly broader [14]. This means apps and websites processing UK residents' tracker health data must be GDPR compliant. Penalties for noncompliance are substantial: up to 4% of company total annual global turnover.

The ICO has the legislative authority to conduct GDPR compliance audits of apps and websites. At the time of our study, it had not audited period trackers. Our UK–based case study audit of three commonly used period trackers, Clue, Flo, and Eve, offers a methodological and conceptual approach aimed at addressing this gap.

2. Materials and methods

2.1. Ethics approval

Our tracker case study was approved by the Kent Law School Research Ethics Approval Group, University of Kent. Study protocol adhered to the Universities UK Concordat to support research integrity [15]. Informed consent was provided by the study participant (a study author) who tested the three selected apps.

2.2. App selection

Women's Health [16] identified Clue, Flo, and Eve as the "best" and the most "popular" period trackers in 2022. Statista [17] listed the three trackers among the most frequently downloaded period tracking apps in 2022–2023. At the time of our study, Flo was preloaded on Apple iPhones. Flo, Clue, and Eve were free at the point of download, though subscription options were available for purchase.

2.3. Methodology

The ICO uses a desk audit methodology [18] to assess GDPR compliance of apps, websites, and data systems. To better replicate the lived experience of period tracker users who input their menstrual cycles, health, mood, and sexual activity data daily, we adopted a user–focused experiential methodology [19] to assess tracker intimate privacy harms and GDPR compliance.

2.4. Audit assessment criteria

We applied GDPR assessment criteria typically featured in ICO audits. The novel aspect of our case study is the development and application of intimate privacy assessment criteria, which we argue responds to an Art. 9 guidance gap. For example, when the ICO audits internet platforms, digital games and apps expected to be used by persons under age 18, a subset of the internationally recognized UK Children's Code (CC) design elements form part of the audit framework [20]. As no similar standardized typology exists for evaluating privacy risks associated with Art. 9 health data processing [21], we developed a set of 15 criteria inspired by Citron's [9] four rules for intimate privacy data protection. Our intimate privacy criteria situate the locus of data privacy tensions on users' inability to negotiate meaningful consent and exercise control over surveillance, marketing, and data sharing (Table 1).

Citron asserts that one's intimate privacy is invaded when others have unwanted access to, and information about, our bodies, minds (thoughts, desires, and fantasies), health, sexual activities and orientation, gender, and the details of our close intimate relationships. This is precisely the type of information users record in their tracker apps.

Zuboff and Véliz [22] identify the importance of digital user ability to monitor, control, and prevent corporate and government surveillance and intrusions. Yet, the deliberate design of digital tracker devices limits users' ability to exercise control. Trackers widen the horizon and scope of data access and accumulation by scooping up personal data. Our intimate privacy criteria privilege surveillance detection and blocking design features, enabling users to exercise their privacy rights. Nissenbaum [23] contends that data flows and privacy protection risk measures need to be contextually appropriate. Building on Waldrum's [24] privacy-as-trust concept, we argue that while the GDPR permits data sharing based on legitimate interest, this blanket permission removes from the user the ability to negotiate the social context for data sharing.

Our study's intimate privacy criteria look for data protection measures that build trust relationships rather than merely police them. Yet, we recognize the saliency of Allen's [25] observation that data regulation measures can be unpopular. One of our criteria, age verification, may meet with parental approval but could be regarded as privacy intrusive (Supplementary Table 1).

2.5. Data collection

Three separate @gmail accounts were used to register the Clue, Flo, and Eve [26] apps under a false name of a female user aged 23. The apps were accessed on an Apple iPhone device and tested for 4 months (March 7 to July 7, 2023). Four actual menstrual cycles were recorded.

Data recording occurred at differing times of the day as this approach best simulated actual usage. Over the 4-month data collection period, no data omissions occurred. Privacy notices were evaluated by two authors who assessed them against GDPR and intimate privacy criteria and observed app performance. The Flesch-Kincaid Grade-Level and Flesch Reading Ease Tests [27] were used to produce privacy notice readability and education-level scores.

Categories pertaining to menstrual matters were similar across the three apps. The range of sexual behaviors, moods, and emotions differed. Where possible, a consistent sexual, mood, and emotional profile pertaining to a 23-year-old university student in a heterosexual relationship was created using a mixture of actual and fake data. This approach meant that in the case of Clue which collected over 30 different sexual behaviors, more categories were left unmarked compared to Flo and Eve which listed fewer behaviors. No photos were loaded into the apps, though Eve encourages this type of information collection. Whereas a fake tracker app identity was used, we did not create fake identity social media sites (FaceBook, Fitbit, and Instagram). No linking to such sites occurred, though we received nudging.

The three apps engaged in nudging and marketing practices. We experienced encouragement to share data across social media platforms, purchase subscriptions, and increase sexual behavior, emotion, and mood data entries. All incidences of nudging, marketing, and subscription upselling were recorded.

As our study focused on free period app use by a UK university student, we did not respond positively to subscription upselling marketing. Nor was the study designed to assess the relationship between dynamic AI and profiling algorithm intensity and the input of sexual activities such as fantasies, anal sex, sex toys, and

Table 1
Case study assessment elements, GDPR, and intimate privacy criteria

	Audited elements	GDPR criteria	Intimate privacy criteria
1	Privacy policy: length, readability, and coverage	Art. 12 Transparent information, readable, easily assessable. Recitals 58–60.	Flesch Readability Test Flesch-Kincaid Education Test Privacy policies covering multiple app versions and websites make it difficult for users to fully understand how their intimate data are processed. Readers will not go to the linked subpolicies.
2	Age verification	Art. 8 Children. Recital 38. ICO Children's Code	Age verification Age–appropriate data collection categories
3	Consent	Art. 5 Data collection must be lawful, fair, and transparent. Recitals 39, 74 Art. 6 Conditions of lawful data processing. Recitals 39–50. Art. 7 Consent. Recitals 32–33, 42–43. Art. 9 Sensitive data processing. Recitals 51–52, 159. Art. 14. Information to be provided when personal data have not been obtained from the data subject. Recitals 60–62. ICO Legitimate interest test	Consent is a process, dynamic, and contextual. Ability to negotiate consent rather than lawful collection on basis of legitimate interest. Dynamic consent for collection of data about third parties. Default: no third-party data collection for those under age 18.
4	Data sharing	ICO Data Sharing Code of Practice ICO Sensitive Data guidance. Privacy and Electronic Communication Regulations 2003 (PECR) requirements are: cookies	Data sharing with explicit consent. Sharing not banned as per Rule 4: Citron. Limited use of legitimate interest.
5	Research (market, product development, and peer-reviewed)	Art 9. Explicit consent. Recitals 26, 29.	Explicit consent for peer-reviewed, market, and app performance research
6	Retention and deletion	Art. 15 Right of access Art. 16 Right of rectification Art. 17 Right to be forgotten Recitals 63–66	Storage on device. Easy to remove data as to add data. User–determined retention periods.
7	Security	Art. 32 Data security practices. Recitals 75–80.	2-Factor authentication Strong passwords No sign-in using social media Strong security measures
8	Accuracy	Art. 5: Data integrity, accuracy, and relevance.	Measures to ensure ovulation accuracy not just track period duration.
9	Anonymity	Not required by GDPR	Default: anonymous mode
10	Data transfer outside of UK/EEA/EU	Art. 3; Art. 44–46. Recitals 101–102, 108–109.	Explicit consent on creation of app for data transfer outside of UK/EEA/EU.
11	Nudging, marketing	Nudging and marketing not explicitly regulated: see legitimate interest Art 6. ICO Children's Code	Explicit, dynamic consent. No default marketing, nudging, and upselling. Adopt CC guidelines for all app users.
12	Cookies	Cookies: PECR	Adopt ICO Guidelines for cookies.
13	Profiling/AI	Art. 22 Recitals 71–72, 91.	Enable users' ability to detect and monitor profiling and use of dark patterns
14	Encryption	Art. 32 Data security practices. Recitals 75–80.	Default encryption for data at rest and in transit.
15	GPS/surveillance	CC Code	Default: no GPS tracing. Surveillance detection software mandatory.

CC, Children's Code; GDPR, General Data Protection Regulation; ICO, Information Commissioner's Office.
GDPR criteria correspond to key GDPR data protection and data subject rights, Articles, and Recitals. Score ratings for each element are shown in Supplementary Table 1.

masturbation, which were categories listed in the apps tested. Nor did we enter mood data suggesting suicidal thoughts or self-harm.

2.6. Statistical analysis

Like ICO audits, we developed a rating system to assess our identified assessment categories (Supplementary Table 2).

At the end of the 4-month test interval, data recorded on an Excel spreadsheet were tabulated. To ensure consistency, inputted tracker assessment values were verified against the criteria.

We scored each app using the ICO traffic-light approach: Green: High Risk Assurance; Yellow: Reasonable Risk Assurance; Orange: Limited Risk Assurance; Red: Very Limited Risk Assurance. We added one additional category: Purple: No Risk Assurance (Supplementary Table 3).

The ICO uses its traffic-light risk assurance rating approach to report overall findings. In our study, the qualifier "Control," which the ICO does not use, was added to our intimate privacy assurance rating to reflect that it is the user who seeks assurance and control. The overall risk assurance rating was calculated by assigning a numerical value (0–4) to each GDPR and intimate privacy assessment category (Supplementary Table 4). This approach allowed us to determine overall similarities and differences between the two criteria assessment systems. No one input category was weighted more than another. The summary risk assessment rating for each assessed category sheds light on each tracker's ability to meet GDPR requirements and reveals the analytical value added by including intimate privacy criteria (Supplementary Table 4).

3. Results

3.1. Overall findings

Compared to summary assessment findings using intimate privacy criteria, GDPR criteria rated the three trackers less harmful. For example, Clue obtained a summary Reasonable Risk Assurance GDPR rating, Flo rated Limited Risk GDPR Assurance, and Eve scored Very Limited GDPR Assurance. When intimate privacy criteria were considered, summary findings were Clue achieved Limited Risk Assurance/Control, Flo attained Very Limited Risk Assurance/

Table 2
Overall risk assurance ratings based on GDPR and intimate privacy criteria

	CLUE	FLO	EVE	RISK ASSURANCE	
				GDPR	INTIMATE PRIVACY
Overall Risk Assurance Ratings				CLUE: Reasonable risk assurance. FLO: Limited risk assurance. EVE: Very Limited risk assurance.	CLUE: Limited risk assurance/ control. FLO: Very Limited risk assurance/ control. EVE: No risk assurance/control.

GDPR (General Data Protection Regulation)

Control, and Eve recorded Minimal Risk Assurance/Control. Lack of negotiable consent, anonymity, encryption, user-determined storage and sharing, and transfer of all UK Flo and Eve users' tracker data to the United States for processing and storage contributed to their lower intimate privacy scores (Table 2).

3.2. Detailed findings

3.2.1. Privacy policy

The GDPR requires privacy policies to be concise, accessible, and readable. Flo and Eve's privacy policies were over 30 pages in length and contained numerous weblinks. Clue's privacy policy was under 10 pages. Flesch Ease Reading scores were mid-range for all three apps. The Flesch-Kincaid Education Test found Clue, Flo, and Clue required college-level education. Length and reading difficulty contribute to user tendency to skip or not read privacy policies, thereby impeding informed decision-making [28]. Such factors compounded by content omissions have significant implications for informed consenting.

3.2.2. User age

Clue, Flo, and Eve require users to meet legal age requirements. Clue, Flo, and Eve state that they will remove data when notified that a user is under age 16.

Apps used in the UK by persons under age 18 must apply the UK CC design code. For this age group, Global Positioning System (GPS) tracking should not be activated by default. Nudging, marketing, and subscription upselling should be blocked. We suggest that the application of the UK CC would require youth access to sexual behavior and mood categories to be age-appropriate. We detected no age verification or parental authorization mechanisms.

3.2.3. Consent

Art. 9 GDPR requires the user to provide explicit, informed consent for data collection and processing. Personal data processing for marketing and app efficiency improvements is permissible based on legitimate interest and contract.

To create a tracker account, the user must tick a box to indicate that they have read the privacy policy. This positive action seemingly fulfills the GDPR requirement for informed, explicit, voluntary consent. We observed no verification of user access to the privacy policy weblink with the result that we could consent without accessing the privacy policy. Clue and Flo enabled users to consent separately to marketing and cookies. To use the app, Eve users must give blanket consent to all activities.

The GDPR provides no user ability to refuse processing based on legitimate interest and contract. Clue and Flo's privacy policies provide a detailed list of legitimate interest and contract processing elements and identify third-party companies involved in app maintenance, quality assurance, and product testing. Eve provided few details. For all three apps, we were not able to negotiate, control, or prevent the processing and sharing of smartphone device metadata and browsing history. Internet Protocol (IP) address and GPS were activated by default.

Our intimate privacy consenting criteria require user ability to negotiate consent, thereby rendering it a dynamic informed process rather than an "all-or-nothing" regime. Users should have the ability to influence intimate data use and sharing authorized by legitimate interest purposes. Results of the required harm test used to determine legality of legitimate interest were not made transparent to the user.

The GDPR requires data collection to be restricted to the minimum amount needed to fulfill the data processing purpose. Clue collected over 30 sexual behavior categories, including fantasies and party nights. Eve encouraged the upload of videos and photos. At the time of our testing, Flo listed 12 sexual activity categories. All user-inputted data, regardless of category, were treated equally when transferred to another country. We observed limited user ability to manage third-party access. Nor could users request category blocking or encryption.

The GDPR does not define explicit consent though it must be freely given, specific, informed, and unambiguous. Nor can it be presumed [29]. Despite a requirement for a higher standard of consent for Art. 9 data processing, apart from Clue which gave the user greater control over research use, the consenting standard used by Flo and Eve placed users into a non-negotiable binary position: agree to the use of your data or not use the tracker. Lacking operationalization of dynamic, negotiated consenting provisions, consent becomes "fictitious" providing an illusion of "moral magic" [8].

3.2.4. Data security

Strong data security features foster trust and ensure effective protection. User anonymity and device data storage permit users to negotiate and control third-party access to intimate information. Only Flo offered an anonymous option. None of the trackers allowed data storage on the device.

3.2.5. Data storage and retention

The GDPR requires users to be informed about data retention and deletion. It should be as easy to remove data as to provide it. We found that Clue and Eve did not specify data retention length. Flo

stated 3 years. All three trackers required the user to request data deletion by email. We were unable to delete historical data using the app, though we could edit current data. Overall, we found weaknesses in all three apps relative to GDPR requirements, and to our intimate privacy criteria which privilege users' determination of data storage mechanisms, retention periods, and data removal procedures.

3.2.6. Data sharing

The GDPR requires consent to use health data for research purposes. Clue provided a high level of assurance for peer-reviewed research. Data security measures such as encryption, data masking, and pseudonymization were used to protect data supplied for research. Flo and Eve did not mention peer-reviewed research. This lack of clarity leaves users uninformed about tracker data research, including whether it occurs or not, and if it does, under what circumstances.

Clue and Flo stated in their privacy policies that legitimate interest and contract, not explicit consent, were used to share tracker data for non–peer-reviewed research such as marketing and quality studies. Eve provided a few details.

Our intimate privacy design criteria demand higher user information and consenting thresholds for peer-reviewed, marketing, and app improvement research. Apart from Clue, insufficient information was provided to users about the types of research studies undertaken and the security measures used to protect data used in peer-reviewed and non–peer-reviewed research.

3.2.7. Prediction accuracy

Three of four menstrual cycles were correctly predicted. The three tested apps are not registered medical devices. The UK National Health Service (NHS) advises against relying on trackers for contraceptive purposes [30].

3.2.8. Nudging, marketing, and cookies

The GDPR does not prohibit nudging and marketing. Our intimate privacy criteria privilege user control of nudging, marketing, and cookies. Clue permitted marketing blocking. Flo and Eve activated subscription marketing every time the app was opened. We encountered inefficient marketing blocking functionality in the Flo app. Eve did not respond to "Do Not Track" blocking attempts. Nudges to increase data entries occurred less frequently for Clue compared with Flo and Eve. We found Clue adopted the Privacy and Electronic Communications Regulations (PECR) cookie requirements in a more diligent manner compared with Flo and Eve.

3.2.9. Surveillance

Our intimate privacy criteria expect location identifiers to be user-determined. All three trackers activated GPS by default. IP address was obtained based on basis of legitimate interest or contract, not consent. No built-in surveillance detection mechanisms were detected.

3.2.10. Data transfer

The GDPR permits territorial transfer of sensitive and personal information [31]. Flo and Eve's privacy policies notify European Union (EU), European Economic Area (EEA), and UK users of diminished legal protections for data transferred outside these jurisdictions. Unless the user carefully reads the privacy policy before creating a Flo or Eve account, they will be unaware that all their data will be transferred to the US for processing and storage. Clue informs users at the time of account creation that their tracker data are processed and retained in Germany. While Flo and Eve's data transfers are GDPR compliant, when the intimate privacy criteria are applied, only Clue attains an acceptable risk rating.

3.2.11. Encryption, AI/profiling

Clue applied encryption to user password and financial information, but not to intimate private data. GDPR Art. 22 requires users to be notified about data profiling. Flo and Eve did not mention profiling, yet observed marketing and nudging suggest it occurred.

4. Discussion

Our experiential case study audit findings indicate that the GDPR alone does not offer an all-inclusive regulatory solution for the protection of sensitive reproductive information processed by period trackers. Application of the study's intimate privacy criteria detected tracker data protection deficiencies not identified by the GDPR and pinpointed harmful tracker device attributes.

For example, we found it worrisome that significant intimate privacy concerns were buried in overly complex and difficult-to-understand privacy policies. UK Flo and Eve users likely fail to recognize that their intimate data will be subject to diminished legal data protections once transferred to the US for processing and storage. Equally concerning is the digital data acquisition occurring without third-party consent. This occurs when users supply information about sexual partners, attach pictures and videos, and enable sharing of interlinked social media apps such as Fitbit and FaceBook.

The ICO 2023 report identified the need to improve tracker privacy policies, yet the matter remains seemingly intractable despite considerable research on the topic [32]. Perhaps we are asking the wrong question. Rather than focusing on privacy policy omissions which lead inevitably to ever-increasing privacy notice complexity as companies endeavor to meet regulator-identified deficiencies, would not implementation of intimate-privacy-by-design offer a possible solution? The challenge then becomes how to accomplish this task in a manner that empowers users but does not create unpopular privacy protection measures.

Our examination of the three most downloaded free trackers shows that they were not designed for youth. Yet research [33] demonstrates that teens under age 18 use period trackers. We argue that greater attention needs to be paid to tracker adherence to the UK CC. The UK *Online Safety Act* 2023 regulations [34] requiring age verification and parental consent will assume greater importance for UK users but will not address other intimate privacy concerns, such as consenting, data transfers, and tracker content scope.

The GDPR and intimate privacy assessment identified consenting regimes requiring users to provide blanket, often uninformed consent. The "all-or-nothing" consent model combined with the ability of tracker companies to rely on legitimate interest to process and share data denies users autonomy to negotiate their tracker data usage. Users are left to rely on inadequate security as their first defence data protection measure. We question why encryption is used for financial information, but not routinely applied to intimate private data.

Consequences of data access are high as trackers can reveal a possible abortion or miscarriage. In the context of UK law, tracker data could indicate that the user misled telemedicine abortion providers about the number of weeks of pregnancy [35]. In cases of sexual assault or spousal abuse, information showing risky or extreme sexual behaviors could be used as evidence.

Our intimate privacy criteria highlight the importance of putting autonomy, control, and choice in the hands of the user. Enabling users to be anonymous, store data on the device, and for apps to provide default data encryption, inclusion of surveillance detection tools, and improved measures for management of marketing, nudging, and data sharing would significantly diminish intimate privacy and data protection risks.

This case study assessment of three popular period apps involved a 4-month observational time-period snapshot of tracker

functionalities as observed by a UK user in 2023. While our study sheds light on nudging and marketing, observations made throughout the entire year would have been a better indicator as Black Friday, Christmas, Valentine's Day, or the user's birthday likely triggers a wave of additional marketing and nudging. We also recognize that dark–patterning techniques fuel Artificial Intelligence (AI) algorithms. Our study was not designed to investigate this technical IT area.

Period trackers map a private landscape of women's innermost lives. While marketing suggests a mere recording of menstrual cycles and related health symptoms, trackers are digital devices documenting and sharing with third parties the user's sexual behaviors, moods, and emotions. The GDPR offers considerable data protections and rights to users. Yet our intimate privacy criteria identified a lack of user ability to negotiate and control intimate data processing and access. This said, we recognize that our intimate privacy-by-design approach is not without challenges. Full implementation of Citron's Rule Four calling for the banning of third-party sharing would be unpopular with IT developers.

Further research, multijurisdictional legal analysis, and multistakeholder commitment are required to transform our case study operational specification of intimate privacy into a comprehensive intimate privacy-by-design standard. While some tracker apps are adopting piecemeal protection measures such as anonymity and device data storage, app developers and regulators adoption of intimate privacy-by-design would provide Femtech device users–enhanced intimate privacy data protection rights.

Author contributions

Pamela M. White: Writing – review & editing, Writing – original draft, Validation, Supervision, Methodology, Data curation, Conceptualization. **Virginia Franqueira:** Writing – review & editing, Funding acquisition, Conceptualization. **Niamh Fuller:** Writing – original draft, Methodology, Investigation, Formal analysis, Conceptualization. **Allison M. Holmes:** Writing – review & editing, Methodology, Conceptualization.

Data availability

All data created during this research are openly available from the Kent Data Repository at https://data.kent.ac.uk.

Acknowledgments

The authors thank the anonymous reviewers of the article and editorial staff of the Contraception Journal for their helpful comments and insightful suggestions.

Appendix A. Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.contraception.2025.111235.

References

[1] (a) Hill K. Deleting your period tracker won't protect you. New Your Times. June 30, 2022. https://www.nytimes.com/2022/06/30/technology/period-tracker-privacy-abortion.html (accessed 16 September 2025). (b) Conti-Cook, Cynthia. Surveilling the digital abortion diary. U Balt L Rev 2020;50:1–77. https://scholarworks.law.ubalt.edu/ublr/vol50/iss1/2 (accessed September 16, 2025).

[2] Gilman ME. Periods for profit and the rise of menstruation surveillance'. Colum J Gend L 2021;41:100–13. https://doi.org/10.52214/cjgl.v41i1.8824

[3] Amelang K. (Not) safe to use: insecurities in everyday data practices with period-tracking apps. In: Hepp A, Jarke J, Kramp L, editors. New perspectives in critical data studies: the ambivalence of data power. London: Palgrave MacMillian; 2022. p. 297–321.

[4] Federal Trade Commission. FTC finalizes order with Flo health, a fertility-tracking app that shared sensitive health data with Facebook, Google, and others. June 22, 2021. 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 (accessed September 15, 2025).

[5] Rampazzo F, Raybould A, Rampazzo P, Barker R, Leasure D. "UPDATE: I'm pregnant!": inferring global downloads and reasons for using menstrual tracking apps. Digit Health 2024;10:1–14.

[6] Kelly BG, Habib M. Missed period? The significance of period-tracking applications in a post-*Roe* America. Sex Reprod Health Matters 2023;31:1–4. https://doi.org/10.1080/26410397.2023.2238940

[7] Solove D. The myth of the privacy paradox. George Wash Law Rev 2021;89:1–52 (accessed September 16, 2025). https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2738&context=faculty_publications.

[8] (a) Solove D. Murky consent: an approach to the fictions of consent in privacy law. Boston Univ Law Rev 2023;104:593–638. https://doi.org/10.2139/ssrn.4333743;
(b) Hurd HM. The moral magic of consent. Legal Theory 1996;2:121–46. https://doi.org/10.1017/S1352325200000434

[9] Citron DK. The fight for privacy: protecting dignity, identity and love in a digital age. New York, NY: W.W. Norton & Company; 2022. p. 156–65.

[10] Worsfold L, Marriott L, Johnson S, Harper JC. Period tracker applications: what menstrual cycle information are they giving women? Womans Health 2021;17:1–8. https://doi.org/10.1177/17455065211049905

[11] Broad A, Biswakarma R, Harper JC. A survey of women's experiences of using period tracker applications: attitudes, ovulation prediction and how the accuracy of the app in predicting period start dates affects their feelings and behaviours. Womens Health 2022;8:1–16. https://doi.org/10.1177/17455057221095246

[12] Privacy International. No body's business but mine: how menstruation apps are sharing your data; 2019. https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruations-apps-are-sharing-your-data (accessed September 16, 2025).

[13] (a) Information Commissioner's Office. ICO to review period and fertility tracking apps as poll shows more than half of women are concerned over data security. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/09/ico-to-review-period-and-fertility-tracking-apps/ (accessed September 16, 2025). (b) Information Commissioner's Office. Understanding the user's experience of fertility and period tracking apps. 2023. https://ico.org.uk/media2/migrated/4029278/understanding-the-user-experience-of-fertility-tracking-apps.pdf (accessed September 16, 2025).

[14] (a) Information Commissioner's Office. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/special-category-data/ (accessed September 16, 2025). (b) https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/02/ico-urges-all-app-developers-to-prioritise-privacy/ (accessed September 16, 2025).

[15] Universities UK Concordat to support research integrity. University of Kent, Kent Law School Research Ethics Approval Group, KLS.Student.004.2022.2023; February 2023. https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Pages/the-concordat-for-research-integrity.aspx (accessed September 3, 2024).

[16] Bradley S, Bacharach E, Martens A. Best period tracker app: 11 options to get to know your cycle, according to ob-gyns. Women's Health Magazine; November 28, 2023. https://www.womenshealthmag.com/health/g26787041/best-period-tracking-apps/ (accessed September 16, 2025).

[17] Statista. Period tracker apps worldwide by downloads. https://www.statista.com/statistics/1307702/top-period-tracker-apps-worldwide-by-downloads/ (accessed September 16, 2025).

[18] Information Commissioner's Office. Audits. https://ico.org.uk/for-organisations/advice-and-services/audits/ (accessed September 16, 2025).

[19] (a) Silverman D. Doing qualitative research. 6th ed. New York, NY: Sage Publications; 2021;
(b) John W, Cresswell JW. Research design: qualitative, quantitative and mixed methods approaches. 2nd ed. London: Sage Publications; 2003.

[20] (a) Information Commissioner's Office. Children's Code. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/ (accessed September 16, 2025). (b) California Children's Data Privacy Act. AB 1949. https://oag.ca.gov/news/press-releases/attorney-general-bonta-essential-legislation-protect-children's-data-privacy (accessed September 16, 2025).

[21] (a) Art 9. GDPR. https://gdpr-info.eu/art-9-gdpr/) (accessed September 15, 2025). (b) Information Commissioner's Office. Sensitive category data guidance. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/special-category-data/ (accessed September 16, 2025).

[22] (a) Véliz C. Privacy is power: why and how you should take back control of your data. London, UK: Penguin Random House UK: Penguin Random House UK; 2020;
(b) Zuboff S. The age of surveillance capitalism: the fight for human future at the new frontier of power. London, UK: Profile Books; 2019.

[23] Nissenbaum H. Privacy in context: technology, policy and the integrity of social life. Redwood City, California: Stanford University Press: Stanford Law Books; 2009.

[24] Waldrum AZ. "Privacy as trust" information privacy for an information age. Cambridge, UK: Cambridge University Press; 2018.

[25] Allen A. Uneasy access: privacy for woman in a free society. Oxford, UK: Oxford University Press; 2011.

[26] (a) 'Clue' (Clue, N/D). https://helloclue.com/ (accessed February 14, 2023). (b) 'Flo' (Flo N/D). https://flo.health/ (accessed February 14, 2023). (c) 'Eve' (Glow, n/d). https://glowing.com/apps (accessed February 14, 2023).

[27] Microsoft 360. Flesch-Kincaid Grade Level Test. Flesh Reading Ease Test. https://support.microsoft.com/en-gb/office/get-your-document-s-readability-and-level-statistics-85b4969e-e80a-4777–8dd3-f7fc3c8b3fd2 (accessed September 16, 2025).

[28] Shipp L, Blasco J. How private is your period? A systematic analysis of menstrual app policy reports. Proc Priv Enhancing Technol 2020;4:491–510. https://doi.org/10.2478/popets-2020-0083

[29] (a) Alaattinoğlu D. Rethinking explicit consent and intimate data: the case of menstruapps. Fem Leg Stud 2022;30:157–179. 10.1007/s10691-021-09486-y. (b) European Data Protection Board guidelines 05/2020 on consent under regulation 2016/679; Plant49 GmbH. Case C-693/17. ECJ Grand Chamber; October 1, 2019. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en (accessed September 16, 2025).

[30] (a) McMillan C. Rethinking the regulation of digital contraception under the medical devices regime. Med Law Int 2023;23:3–25. 10.1177/09685332231154581. (b) National Health Services. Natural family planning. https://www.nhs.uk/contraception/methods-of-contraception/natural-family-planning/ (accessed September 16, 2025).

[31] (a) EU Standard Contractual Clauses Art. 46. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en (accessed September 16, 2025). (b) Corporate Binding Rules. ICO. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/guide-to-binding-corporate-rules/a-uk-bcr-addendum/. (accessed September 16, 2025).

[32] Slepchuk AN, Milne GR. Informing the design of better privacy policies. Curr Opin Psychol 2020;31:89–93. https://doi.org/10.1016/j.copsyc.2019.08.007

[33] Fowler LR, Gillard C, Morain S. Teenage use of smartphone applications for menstrual cycle tracking. Paediatrics 2020;145:1–3. https://doi.org/10.1542/peds.2019-2954

[34] UK Online Safety Act 2023. Ofcom Quick Guide to Children's Safety Codes. https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/quick-guide-to-childrens-safety-codes/ (accessed September 16, 2025).

[35] R v Foster [2023] EWCA Crim 1196; Royal College of Obstetricians and Gynecologists. RCOG issues guidance for healthcare professionals on involving the police following abortion and pregnancy loss. 22 January 2024. https://www.rcog.org.uk/news/rcog-issues-guidance-for-healthcare-professionals-on-involving-the-police-following-abortion-and-pregnancy-loss/ (accessed September 16, 2025).