THE ILLUSION OF CONSENT: A CASE STUDY OF THE FLO APP AND THE EXPLOITATION OF WOMEN'S REPRODUCTIVE DATA UNDER MODERN DATA PROTECTION FRAMEWORKS

Simran Shokeen, LLM (IPR & Tech) O.P. Jindal Global University

Srishti Singh, LLM (IPR & Tech) O.P. Jindal Global University

ABSTRACT

This paper examines the case of Flo Health, Inc., the developer of one of the world's most popular period and fertility tracking applications, as a lens through which to critique the adequacy of existing data protection frameworks in safeguarding sensitive reproductive health data. Drawing on the 2021 Federal Trade Commission (FTC) settlement with Flo Health, the paper argues that the consent mechanisms deployed by digital health platforms constitute a structural illusion—formally valid but substantively hollow. Through an analysis of the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the post- Dobbs regulatory environment in the United States, this paper contends that current frameworks are ill-equipped to address the unique vulnerabilities created by the commodification of intimate bodily data. The paper concludes by proposing doctrinal and regulatory reforms necessary to render meaningful protection for users of femtech applications.

1. Introduction

The proliferation of so-called femtech, or a portmanteau of technologies, purportedly to serve the health needs of women, has helped to establish a multi-billion dollar business, centered around intimate disclosure. Flo, Clue, and Glow are the applications that encourage users to record menstrual periods, sex life, mood swings, pregnancy, and miscarriages. Such platforms put data sharing into contextualisation as a demand towards personalised health information, where consent is embedded within the dark, multi-layered privacy terms and conditions, which the average consumer does not read and cannot meaningfully comprehend.

The case of Flo Health that was settled with the FTC in January 2021 suggested some innate resistance to the very beginning of the existing data protection laws: the discrepancy between the form and the reality of consent. "The privacy policy of Flo promised the users that their health data would be kept highly confidential, but at the same time, it sent comprehensive reproductive data to the advertising analytics tool by Facebook and Google Analytics. This policy-meets-practice paradox reveals the futility of consent-based regulation systems in a commercial surveillance economy in terms of sensitive health information[1].

2. The Flo Case: Facts, Settlement, and Broader Context

2.1 Factual Background

Flo Health is a period tracking app that was founded in Belarus in 2015 and is based in London and has over 230 million registered users as of 2023 (Flo Health, 2023)[2]. The key premise of the app, cycle forecasting through machine learning, means that the user will have to provide more details of reproductive information, including the date of the period, sexual intercourse, birth control use, fertility treatments, and pregnancy outcomes.

In 2019, The Wall Street Journal published an investigation that disclosed a flow involving user health data to Facebook Software Development Kit (SDK) which contained cues on when someone was menstruating or attempting to conceive (Schechner and Secada, 2019)[3]. This

[1] Jack M Balkin, 'The Fiduciary Model of Privacy' (2020) 134 *Harvard Law Review Forum* 11
[2] Flo Health, 'Flo Period & Ovulation Tracker' https://flo.health accessed 10 April 2026
[3] Sam Schechner and Mark Secada, 'You Give Apps Sensitive Personal Information. Then They Tell Facebook' *The Wall Street Journal* (22 February 2019)

transmission was despite Flo giving explicit privacy guarantees and apparently against Facebook developer policies, which forbade sharing sensitive health information.

2.2 The FTC Settlement

In January 2021, the FTC resolved with Flo Health under Section 5(a) of the Federal Trade Commission Act that prohibits unfair or deceptive acts or practices. The settlement placed no monetary penalty on the settlement- a fact that attracted a lot of criticism by the consumer advocates. Flo had to, instead, secure positive express consent of the users of the health information before disclosing health data to third parties, inform users about the information shared with them and direct third parties to delete the unlawfully obtained information (FTC, 2021).

The non-punitive nature of the settlement was an indication of the limited statutory powers of the FTC at that time and an example of what Solove and Citron (2022) term as the regulatory gap in the US health data law: the irrelevance of the Health Insurance Portability and Accountability Act (HIPAA) to non-covered parties, like app developers. Given that Flo is a commercial technology business, rather than a healthcare provider or a health insurance company, it was well outside the bounds of HIPAA protection, and so subjected to the general consumer protection law, which is evidently unsuitable in the context of the sensitivity of the data involved.

3. The Illusion of Consent: Structural Deficiencies in Data Protection Frameworks

3.1 Consent Under the GDPR

The most comprehensive data protection tool in the world is the General Data Protection Regulation that is followed in the European Union (Regulation (EU) 2016/679). Article 9 GDPR classifies data as concerned with health as a special category, the processing of which is not only unlawful in principle but also can be only justified in strictly defined cases, e.g., express consent, which is encompassed in Article 9(2)(a). The explicit consent should involve an affirmative act that is free, specific, informed, and unambiguous (Article 4(11) GDPR).

In reality, though, the architecture of consent implemented by femtech applications subverts such requirements systematically. Zanfir-Fortuna (2020) notes that there are three pathologies in a structure. First, there is consent bundling: a combination of multiple purposes of

processing, within the framework of a single consent request, and conceals the identity of the data shared with the advertising networks, and the risk profile. Second, dark patterns: interface design decisions that steer users to wide consent and shun privacy-protective decisions. Third, information asymmetry: the abuse of legalistic and lengthy privacy policies that on paper comply with the transparency requirements of the GDPR but in reality fail to do so.

Guidelines on consent introduced by the Article 29 Working Party (since replaced by the European Data Protection Board (EDPB, 2020)) recognise these pathologies but have been challenging to implement in the context of mobile apps with operations spanning several jurisdictions. The record of the Irish Data Protection Commission in enforcing its rules on large technology companies evidences the structural challenge of imposing accountability on platform companies through a one-stop-shop system that vests oversight power in the country of the establishment of the data subject[4].

3.2 The CCPA and Sectoral Gaps in US Law

The California Consumer Privacy Act of 2018 (with the California Privacy Rights Act 2020 appended)[5] is the strongest state-level data protection framework in the United States providing strong data protection frameworks. The CCPA grants access to information about what personal data is being gathered to California residents, the right to delete and to opt-out of selling personal information. The California Privacy Rights Act, which is an addition to these rights, entailed specifications on sensitive personal information, of which the category of personal information which health of a consumer falls under is entailed.

However, despite the framework, CCPA has fewer chances to succeed in the femtech environment due to several reasons. The enforcement mechanism of the statute is mainly reactive, based on complaints to the California Privacy Protection Agency or individual litigation based on a limited, private right of action which is confined to data breach cases. More fundamentally, the opt-out model of the CCPA (as opposed to the opt-in model in the GDPR), makes the data subject the responsibility of protection rather than the data controller, which is the opposite of how protection ought to be shared in the case of intimate health information (Calo and Rosenblat, 2017).

[4] Jack M Balkin, 'The Fiduciary Model of Privacy' (2020) 134 *Harvard Law Review Forum* 11
[5] California Consumer Privacy Act of 2018, Cal Civ Code § 1798.100 et seq (as amended by Cal Prop 24, 2020)

3.3 The Problem of Contextual Integrity

A good analytical framework to develop the reasons behind why the ethical implications of sharing reproductive data are not evident in formal consent is provided by the theory of contextual integrity of Helen Nissenbaum.the norms of privacy are relative: the information flows in the right way when the norms of the situation in which data was first revealed are followed. When sharing menstrual data with a health application, users do it in the medical context, where there are norms of confidentiality and restricted disclosure. Such information transfer to the advertising platform of Facebook does not violate contextual integrity since users did not express their consent in any technical sense but because the stream of information violates the unwritten principles of the health context[6].

This discussion indicates an inherent failure of consent-based models: they are interested in the time of revelation, as opposed to the continuous stream and the application of information. The customer who agrees to the terms of service of Flo in no meaningful sense knows what will become of their data down-stream in the complex web of data brokers, advertising networks, and analytics services, to which their data might be sold. They have time-temporal and cognitive constraints to such an extent that they cannot be formalized in legal agreement.

4. Reproductive Data in the Post-'Dobbs' Environment

In June 2022, the US Supreme Court's Dobbs v. Jackson Women's Health Organization, 597 U.S. 215 (2022)[7] ruling, which struck down the federal constitutional right to abortion, fundamentally changed the stakes of reproductive data collection, legally. A possible source of evidence of criminal activity in states where abortion has been criminalised or severely restricted is the reproductive information in the femtech applications. In multiple states, prosecutors have already requested health information during their investigations concerning abortion (Hao & Brakman Reiser, 2022)[8].

Flo, a case that pre-dates Dobbs, was a case that was litigated under a regulatory context where reproductive information was commercially sensitive, but not legally hazardous. Since Dobbs,

[6] Daniel J Solove and Danielle K Citron, 'Risk and Anxiety: A Theory of Data-Breach Harms' (2022) 96(4) *Texas Law Review* 737
[7] *Dobbs v Jackson Women's Health Organization* 597 US 215 (2022)
[8] Kashmir Hao and Dana Brakman Reiser, 'Period Tracking Apps and the Threat to Reproductive Privacy after Dobbs' (2022) 52(5) *Hastings Center Report* 9

the same information has acquired the potential criminal evidentiary value. Period tracking information regarding a missed period followed by a later entering an irregular cycle can be used in a restrictive jurisdiction to suggest an abortion. This potential turns the harm model that femtech data protection is based on into a potential tool of state surveillance and criminal prosecution.

The existing data protection models are not suitable in this new risk environment. Neither the harm-reduction paradigm of the GDPR nor the consumer rights paradigm of the CCPA was aimed at covering the usage of commercial health data in the criminal process. The law enforcement gaining access to data stored by commercial entities is largely controlled by the Electronic communications privacy Act (1986) and the Stored communications act that have been developed before the advent of smartphones, cloud storage, or period tracker apps. These frameworks provide lax requirements of government access to data stored, especially by subpoena that lacks the same judicial scrutiny as a warrant (Ghosh, 2021)[9].

5. Comparative and Reform Perspectives

5.1 The Limits of Transparency-Based Regulation

The prevailing regulatory reaction to data exploitation that has been improved transparency requirements has proved to be not effective in the femtech setting. The transparency requirements which are both modelled in the GDPR (Articles 1314)[10] and the disclosure requirements of the CCPA are premised on the assumption that informed users can make independent decisions about data sharing. This is an assumption that is challenged empirically. Empirical studies have persisted in demonstrating that privacy policies are never read by the users and even when they are read, the cognitive burden of comprehending it is too much to impose on a lay person.

A slightly improved method of regulation will be to restrict the purpose to which sensitive health data can be used, without consent. The proposed EU Health Data Space Regulation (2022) takes the direction of this approach and purpose limit is fixed as a strict constraint of secondary processing of health information and is not a default around which users can agree

[9] Dipayan Ghosh, *Terms of Disservice: How Silicon Valley Is Destructive by Design* (Brookings Institution Press 2021)
[10] General Data Protection Regulation (EU) 2016/679

to be diverted. Similarly, the American Data Privacy and Protection Act that was proposed in 2022 would not permit data minimisation exceptions on sensitive data like reproductive health data.

5.2 Structural Remedies

Along with the changes in the doctrines, the Flo case is a pointer to the fact that structural interventions within the data economy are needed. Zuboff (2019) asserts that, as the economic model that relies on the mining and selling of behavioral information, surveillance capitalism cannot be adequately counterbalanced through the individual consent, because the concept of consent presupposes the autonomy that surveillance capitalism is systematically abiding by. Within this context, the successful protection of reproductive data should not only entail improved consent practices but also limitations of business paradigms that make data exploitation a viable economic opportunity".

5.3 The Adequacy of the FTC Settlement Revisited

The 2021 settlement that FTC has made with Flo Health must be evaluated against these structural standards and fail. The absence of monetary penalties, the limitation of relief to the standards of potential conduct, and the absence of personal notification to injured users (as in the initial proposal) are symptomatic of the fewer legal resources of the FTC and not a considered ruling as to a commensurate penalty. The following FTC order of 2023, which also requires Flo to seek independent privacy audits and raise user notification requirements, can only be described as a minor step forward but in fact reactive, rather than deterring in nature (FTC, 2023).

The difference between European enforcement is educative. In 2022, the French data protection regulator, CNIL, fined Google (150 million) and Facebook (60 million) due to violating the French version of the ePrivacy Directive on cookie consent mechanisms, which in its turn is not as heinous as the wholesale transfer of reproductive health information to advertisers. This difference in the strength of enforcement would be structural difference in the capacity of regulation and political will and not difference in the normative intensity of the underlying behavior[11].

[11] Gabriela Zanfir-Fortuna, 'The Limits of Consent in the GDPR' (2020) 6(2) *European Data Protection Law Review* 214

6. Conclusion

The Flo Health case exemplifies a more systemic problem in femtech, in which sensitive reproductive information is gathered in the name of consent and deployed in the black-box business environments. This forms a misleading appearance of agreement, with the regulatory structures that emphasise formal disclosure over actual user autonomy. Such practices are extremely dangerous in the post-Dobbs context, with reproductive data potentially subjecting people to legal repercussions. This is an issue of civil liberties and bodily autonomy as the current regulations on data protection do not offer sufficient protection. Proper reform must include restrictions on purpose, prohibition of health data advertisements, fiduciary, enforcement, and a full scale federal privacy law.