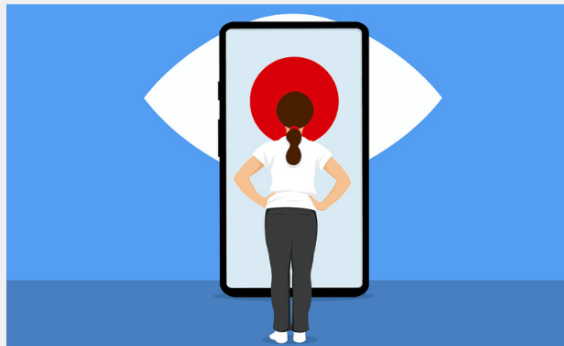


# Intimate Data, External Access: Period Tracking Apps' Privacy Challenges

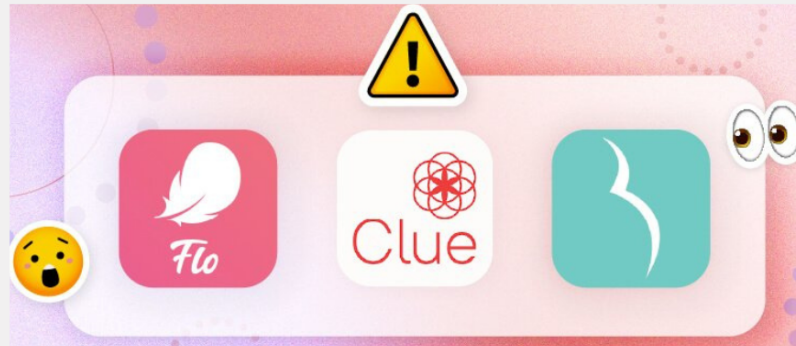
Anupama Bhatta  
University of Michigan School of Information (UMSI)

## Introduction & Case Background



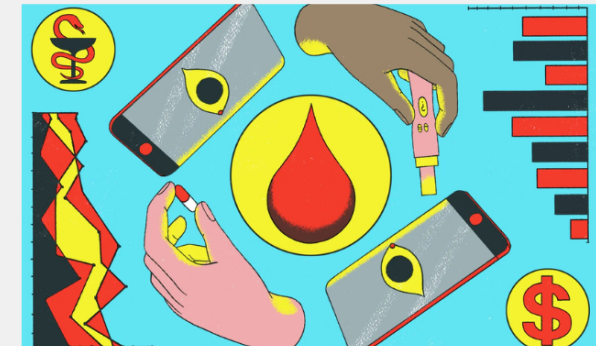
Privacy surveillance concerns with period tracking apps.  
Illustration: Kiersten Essenpreis for Consumer Reports (2022)

## Ethical Dilemma: Privacy vs. Profit



Mozilla's 'Privacy Not Included' rating of popular period tracking apps showing privacy risk levels.  
Source: Mozilla Foundation (2022)

## Key Recommendations



Data monetization concerns with period tracking apps.  
Source: Bloomberg

### From Intimate Data to Privacy Breaches

- Period tracking apps used by 200+ million women to collect intimate health data
- In 2019, WSJ revealed Flo shared data with Facebook/Google despite privacy promises
- FTC settlement highlighted gap between privacy claims and practices
- Period tracking apps collect extensive sensitive data: cycle dates, sexual activity, fertility plans, physical symptoms, and emotional states
- Mozilla Foundation found 18 of 25 reproductive health apps failed to meet basic privacy standards
- Users report feeling "victimized" and "violated" after learning of data sharing (FTC, 2021)

### Conflicting Values and Stakeholder Interests

- Users face "privacy paradox": Need health tools but must surrender intimate data
- Apps employ "data first, then consent" models (Mozilla, 2022)
- Post-Roe concerns: Data could potentially be used in legal investigations
- App developers claim to empower women's health while monetizing intimate data
- Data brokers receive "vital" health data for marketing purposes without users' meaningful consent (Frasco v. Flo Health, 2021)
- European GDPR provides stronger protections than current U.S. regulations (Clue, 2025)
- Regulatory bodies like FTC have limited enforcement mechanisms for sensitive health data

### Toward Ethical Data Stewardship

- Implement local device storage instead of cloud servers
- Establish reproductive health data as protected category
- Require standardized privacy safeguards (encryption, minimal retention)
- Center business models on user welfare over data exploitation
- Privacy-focused alternatives like Euki store data locally and offer stronger protections (Mozilla, 2022)
- Promote education on privacy implications and protection strategies that empower users to make informed choices about their reproductive health data (Hammond & Burdon, 2024)