Menstrual Metrics

An Analysis of Privacy and Security in Menstrual Health Tracking Applications

Alex (Alexandrina) Hanam[1]
Faculty of Information and Media Studies, University of Western Ontario

Introduction

I completed research on the privacy and security measures of smartphone apps and wearable computing that track menstrual health.

Why did I do it?

1. Personal curiosity and concern; I use one!
2. Clarity; data management by apps is largely unknown and misunderstood[2]
3. Reproductive and menstrual health needs to be talked about aka feminism

How did I do it?

I looked at two smartphone apps and one app-wearable device combo: Clue, Glow, and LEAF.

Questions asked:

- What security measures are in place?
- What are they telling their users?
- What details are shared or omitted?
- What are the consequences?

Legislation

Legislation regarding personal health data depends on the geographic location of the server that stores the information.

- *PIPEDA*
- *Digital Privacy Act* amendments
- Provincial legislation
  eg: Ontario's *PHIPA*, Alberta's *PIPA*

- Legislation per country and between members of European Union
- Effects of Brexit unknown

- Privacy legislation at state level with a patchwork understanding and application[7]
- *HIPAA* does not apply to devices not administered by a physician or hospital[8]

US Supreme Court rulings (1976, 1979) set precedent that there is "no legitimate expectation of privacy in information that is voluntarily turn[ed] over to third parties."[9]

Informed consent is VITAL.

Summary For Developers:

- Provide a copy of privacy policies and Terms of Service in language that is clear and accessible.
- Ask for access to specific data or smartphone functions on an as-needed basis and explain how it affects the app's use.

App Analysis

Clue[3]

+ stores health data separate from identifiers
+ encrypted transmission from app to server
+ authentication & remote erasure
+/— synchs data with FitBit
+/— shares (anonymized) data with third parties

Glow[4]

+ firewalls & data encryption
— auto acceptance of policy
— retains personal & financial info even if account is deleted
— data shared with unspecified third parties
— data breach in 2016[5]

LEAF[6]

+ outlines user rights
— unclear policy application
— data shared with unspecified third parties
— users must consent to data being transferred outside of their country

Privacy Policies

App stores don't require developers to include a privacy policy or provide one in accessible language. In one study 32% of health apps didn't provide either option.[10]

Users do not read these policies and are not aware of what happens with their data. This is not informed consent.

92% of health tracking apps use unencrypted data storage.[11]

24% of health tracking apps transmit personal data without informing the user.[12]

An estimated 1.5 billion people will be using health tracking apps or devices by 2018.[13]

Personal data cannot be copyrighted because it consists of facts, not creations or expressions.[14]

Summary For Users:

- Learn how to read privacy policies and Terms of Service.
- Read through app prompts before accepting them.
- Look up security protections in place within apps.
- Email an app developers for clarification on policies that explain exactly how personal data is going to be used
- Be proactive and learn more about your personal digital security.

References
1. Feel free to contact me at ahanam@uwo.ca
2. Chen, Juliana, Adrian Bauman, and Margaret Allman-Farinelli. "A Study to Determine the most Popular Lifestyle Smartphone Applications and Willingness of the Public to Share their Personal Data for Health Research." *Telemedicine and e-Health* (2016). doi:10.1089/tmj.2015.0159
3. "Privacy Policy for Clue: Period and Ovulation Track for iPhone and Android." *HelloClue.com*. http://helloclue.com/privacy.html
4. "Glow - Privacy." *Glow, Inc.* https://glowing.com/privacy
5. Beilinson, Jerry. "Glow Pregnancy App Exposed Women to Privacy Threats, Consumer Reports Finds." *Consumer Reports* (July 28, 2016). http://www.consumerreports.org/mobile-security-software/glow-pregnancy-app-exposed-women-to-privacy-threats/
6. "Privacy - Bellabeat." *Bellabeat.com* https://webshop.bellabeat.com/pages/privacy
7. Becker, Bernd W. "The Quantified Self: Balancing Privacy and Personal Metrics." *Behavioral & Social Sciences Librarian* 33 (2014): 212-5.
8. Cha, Ariana Eunjung. "The Revolution Will be Digitized." *The Washington Post*, May 9, 2015. http://www.washingtonpost.com/sf/national/2015/05/09/the-revolution-will-be-digitized/
9. *Smith v. Maryland* 1979 as quoted in Becker, "The Quantified Self," 214.
10. Dehling, Tobias, Fangjian Gao, Stephan Schneider, and Ali Sunyaev. "Exploring the Far Side of Mobile Health: Information Security and Privacy of Mobile Health Apps on iOS and Android." *JMIR mHealth and uHealth* 3, 1(2014): e8. doi:10.2196/mhealth.3672.
11. Dehling et al.
12. Dehling et al.
13. Huckvale, Kit, José Tomás Prieto, Myra Tilney, Pierre-Jean Benghozi, and Josip Car. "Unaddressed Privacy Risks in Accredited Health and Wellness Apps: A Cross-Sectional Systematic Assessment." *BMC Medicine* 13, 1 (2015): 214-227. doi:10.1186/s12916-015-0444-y
14. Ball, Madeleine. "QS Access: Personal Data Freedom." *QuantifiedSelf.com*, February 11, 2015. http://quantifiedself.com/2015/02/qs-access-personal-data-freedom/