August 6, 2020

Federal Trade Commission
Division of Privacy and Identity Protection
600 Pennsylvania Avenue NW
Washington, DC 20580

Re: Premom's Deceptive Privacy Practices Places Vulnerable Users' Data at Risk

Dear Ms. Mithal,

On behalf of the International Digital Accountability Council ("IDAC"), a non-profit international watchdog organization dedicated to improving the digital ecosystem, we write to raise with you concerns that have emerged from the recent investigation our team of technologists and lawyers recently conducted into the digital privacy practices of Premom, a fertility mobile application ("app") found in the Google Play Store and Apple App Store.

Launched in 2017, Premom is an app "dedicated to helping women get pregnant quickly and naturally."[1] Owned by Easy Healthcare Corporation (formerly Easy At Home Medical LLC), and based in Burr Ridge, Illinois, their app acts as an ovulation tracker, period calendar, and fertility companion. Premom's Facebook group currently has 32,000 members[2] and the app has been downloaded over 500,000 times as of November 2019.[3]

Our investigation has led us to be concerned that Premom may be engaged in deceptive practices as defined in the Federal Trade Commission Act. In particular, we believe there are material differences between what Premom states in its privacy policies and what our technical tests reveal. Our findings and concerns are outlined as follows.

1. Premom has two separate privacy policies that are not consistent with each other.

Premom currently has two separate privacy policies that are mutually inconsistent with each other. Their website privacy policy (last updated May 2017) differs from their in-app privacy policy (last updated April 2019). These privacy policies differ in their disclosures around the type

[1] https://premom.com/
[2] https://www.facebook.com/groups/PregnantwithPremom/
[3] https://premom.com/pages/about-us

of personal data Premom collects and shares with third-parties, resulting in confusion and inconsistency.

Of particular concern, the website privacy policy fails to mention that Premom collects location data from users.[4] Users typically read website privacy policies, as opposed to in-app privacy policies. Here, users cannot rely on the disclosures in the in-app privacy policy because by the time they have downloaded the app and read the in-app privacy policy, their location has already been collected.

2. Premom appears to be secretly sharing geolocation data and device identifiers with third-parties, including untrustworthy companies, without disclosure, contradicting their own privacy policies.

We observed Premom sharing user geolocation data and non-resettable device hardware identifiers to third-parties, including Jiguang, Umeng, and UMSNS, without disclosure.

This data-sharing practice is not disclosed in either of Premom's privacy policies. Indeed, it contradicts Premom's representations that Premom will not share users' personal information with third-parties without user permission. Sharing this type of personal data exposes users to an array of privacy risks, including long-term and persistent tracking across multiple devices and apps, profiling, and unwanted targeted advertising. We observed the following occurring:

- Jiguang is collecting on Android devices:
    - Geolocation
    - Router MAC Address (surrogate for location)
    - Android Advertising ID (AAID)

- UMSNS is collecting on Android devices:
    - Android ID (Google Play Terms disallows use of Android ID for advertising purposes[5])
    - HWID (hardware identifier tied to the device)
    - IMEI (hardware identifier tied to the device)
    - Wi-Fi MAC Address (hardware identifier tied to the device)

- Umeng is collecting on Android devices:
    - Android Advertising ID[6]
    - Android ID (Google Play Terms disallows use of Android ID for advertising purposes)
    - HWID (hardware identifier tied to the device)
    - IMEI (hardware identifier tied to the device)
    - Wi-Fi MAC Address (hardware identifier tied to the device)

[4] https://premom.com/pages/privacy-policy
[5] https://support.google.com/googleplay/android-developer/answer/6048248?hl=en
[6] Google Play Developer Policies prohibit connecting the Android Advertising ID "to personally-identifiable information or associated with any persistent device identifier (for example: SSAID, MAC address, IMEI, etc.) without explicit consent of the user."

- Bluetooth Name
- Bluetooth MAC Address
- Geolocation
- Router SSID (network name and surrogate for location)
- Router MAC address (surrogate for location)

Tests by IDAC reveal that Jiguang's Android push-notification software development kit ("SDK") -- called JPush -- discreetly collects users' personal data. Jiguang, a Chinese mobile developer and analytics provider, appears to go to great lengths to obfuscate its practices. The JPush SDK continually collects location, persistent identifiers, and lists of all the other apps installed on a user's device -- all without the user's knowledge. There is no clear and simple method for users to stop this practice from occurring.

Umeng, owned by Alibaba, is a Chinese mobile app analytics provider. Umeng's Android SDK is also aggressive in its data collection practices, based on tests conducted by IDAC. There, we observed Umeng's SDK collecting the Android Advertising ID, Android ID, device serial number, MAC address, Wi-Fi router's MAC address, and Wi-Fi router's name (Service Set Identifier).

Both of Premom's privacy policies state:

> ***We will not share your personal information with any other third parties without your permission****, unless: (a) we are required to do so by law or when necessary to comply with a current judicial proceeding, a court order or legal process served on the Company. In all cases, such information will only be disclosed in accordance with applicable laws and regulations, and/or (b) in the event of a sale, merger, liquidation, dissolution, reorganization or acquisition of the Company so long as the party acquiring the information agrees to be bound by the terms of this Privacy Policy.*

Additionally, Premom's website privacy policy states:

> *Notwithstanding, you explicitly consent to the following use by us and disclosure by us of your information:*
>
> - *Obtaining and tracking your usage and **nonidentifiable information** of you pertaining to the application for the purposes of tracking analytics of the usage of our application, including sharing information with analytic software extensions provided by third parties*
> - *Obtain **nonidentifiable data** about you, compile that data with the nonidentifibale data of other users, and disclose that information to third parties.*

Our investigation suggests that both of these statements are untrue because Premom is sharing personal information with third-parties. Non-resettable hardware identifiers are personally identifiable information because they are tied to a user's device and it is almost impossible for a user to reset them or erase their digital footprint, thereby allowing companies with this

information to infer who the individual users are. Additionally, by sending multiple device identifiers and geolocation data together, third-parties can infer who Premom's users are.

There is no clear evidence that Premom's data sharing practices fall into the exceptions outlined in their own privacy policies. Premom has not been forthcoming with their third-party data sharing practices. Users are not aware that their sensitive information has been shared with untrustworthy third-parties. Sharing precise geolocation data and non-resettable hardware identifiers with third-parties is not required for Premom to provide the services it advertises to users.

3. Premom engages in ID bridging, violating Google's Developer Policies.

Premom's in-app privacy policy states that Premom collects "IDFA (Identifier for advertisers), Android ID (in Android devices), Google Advertiser ID, Customer issued user ID and other similar unique technical identifiers." Our tests also reveal Premom sending these identifiers together to the third-parties noted above. Collecting the Android ID, Android Advertising ID ("AAID"), and other persistent device identifiers together results in the prohibited practice of ID bridging, which allows the app to circumvent Google's privacy controls and persistently track users across apps. Google's Developer Policies specifically state, "The advertising identifier must not be connected to personally-identifiable information or associated with any persistent device identifier (for example: SSAID, MAC address, IMEI, etc.) without explicit consent of the user."[7] Disclosing this in its in-app privacy policy does not necessarily mean the user has provided their explicit consent.

4. Premom's representation to users that collecting lists of installed apps for functionality purposes is questionable.

Premom obtains and tracks, "[y]our inventory of installed applications to permit our application to properly function."[8] The assertion that obtaining and tracking an inventory of a user's installed applications is necessary for Premom's app to properly function is highly questionable. Moreover, collecting lists of installed apps on users' devices can reveal a tremendous amount of sensitive personal information about users including their sexual orientation, religious affiliations, and political leanings. Premom can infer information about users through this app inventory collection practice and subsequently create profiles for advertising and tracking purposes.

[7] https://support.google.com/googleplay/android-developer/answer/9904549

[8] According to Premom's website privacy policy, Premom also collects, "social media account names, authentication information, inventory of installed applications on Your device, phonebook or contact data, microphone and camera sensor data, sensitive device data, and other information." Although this data collection is disclosed, this blanket collection practice goes against the widely-recognized privacy principles of data minimization and proportionality.

5. Conclusion

Thank you for your attention to this matter. We would be happy to answer any questions you may have and to provide further documentation upon request. We are also sharing these concerns with the Illinois Attorney General and Google. Please do not hesitate to contact us at info@digitalwatchdog.org if we can be of any further assistance.

Sincerely,

Quentin Palfrey
President, IDAC

Lena Ghamrawi
Chief of Staff/Policy Counsel, IDAC