Device Identifiers: When Data Collection Gets Personal

September 9, 2020 Tim Newman, Jennifer Kreick

PRACTICES Healthcare and Life Sciences, Precision Medicine and Digital Health, Privacy and Cybersecurity

On August 28, a bipartisan contingent of U.S. Senators sent a letter (the "Letter") to the Federal Trade Commission ("FTC") requesting an investigation and agency guidance into the allegedly deceptive practices of the digital health mobile application, Premom.[1] The Letter seeks the FTC's guidance pertaining to Premom's consumer data collection and sharing practices. The FTC's anticipated response could impact digital health companies and other digital technology companies.

Premom is a pregnancy planner mobile application that tracks fertility, ovulation, and other personal health data to "help[] women get pregnant quickly and naturally."[2] The letter alleges that Premom shared its users' personal data with third-party advertising companies without the users' consent and contrary to Premom's own privacy policy. Specifically, the letter states that while Premom's privacy policy claimed the app only shared "nonidentifiable" information, Premom collected and shared its users' non-resettable device hardware identifiers with three companies.[3] Non-resettable device hardware identifiers are a category of device-specific data that include, for example, a device serial number, an International Mobile Equipment Identity (IMEI) number, geolocation, and "Advertising ID."

According to a letter from watchdog organization International Digital Accountability Council ("IDAC") referenced in the Letter, 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."[4] The Letter asks the FTC to examine whether Premom's alleged conduct violated Section 5(a) of the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce."[5] Chiefly, the FTC is faced with the question of whether it considers non-resettable device hardware identifiers to be "personally identifiable information," subject to consumer privacy protections.[6]

While the FTC has not specifically addressed whether non-resettable unique user device identifiers are personally identifiable, prior FTC enforcement actions may be instructive. For example, in 2015, the FTC settled with Nomi Technologies over allegations that the company misled consumers regarding its tracking technology. According to the FTC's complaint, Nomi tracked and collected persistent hardware identifiers from consumers that walked into or passed by its customers' retail stores. Nomi's privacy policy promised consumers that it would provide an opt-out mechanism at stores using its tracking technology, and this promise implied that consumers would be informed when stores were using Nomi's tracking services.[7] The FTC alleged that the promises were not true because no in-store opt-out mechanism was available, and consumers were not informed when the tracking technology was in use.

While there remains some uncertainty in the sphere of consumer data collection, digital health companies can take the following steps to avoid inadvertent noncompliance with the FTC Act:

- Update privacy policies to accurately and consistently reflect data collection and sharing practices across all platforms, and regularly review privacy policies to ensure they account for any changes in the company's operations.
- Ensure users are provided with clear and unambiguous notice any time their data is being collected, and particularly when it is being shared with third parties in any identifiable (whether on the consumer level or device level) form.
- Provide readily accessible and navigable options for users to opt-out of or revoke consent for sharing personal data (which may include non-resettable hardware identifiers).
- Consult attorneys with expertise in consumer privacy, particularly in managing health data, to review your privacy policy and data sharing practices.

For questions regarding this article or digital health matters, please contact one of the authors or a member of our Healthcare and Life Sciences or Precision Medicine and Digital Health practice groups.

---

1. Letter from United States Senators Amy Klobuchar, Jerry Moran, Maria Cantwell, Shelley Moore Capito, Richard Blumenthal, Elizabeth Warren, and Mark R. Warner to the Hon. Joseph J. Simons, Chairman of Fed. Trade Comm'n (Aug. 28, 2020), https://www.capito.senate.gov/imo/media/doc/21CB6CC23B42B9A1BCE0C4076F467E2E.082820ftcpremom.pdf

2. PREMOM HOMEPAGE, www.premom.com (last visited Sept. 4, 2020).

3. One of the third-party companies allegedly attempted to conceal the data transmissions it was receiving from Premom, further raising suspicion regarding Premom's data-sharing practices. Letter from Int'l Digit. Accountability Council to the Fed. Trade Comm'n at 3 (Aug. 6. 2020), https://digitalwatchdog.org/wp-content/uploads/2020/08/IDAC-Federal-Trade-Commission-Letter.pdf [hereinafter IDAC Letter].

4. IDAC Letter, supra note 3, at 3-4.

5. 15 U.S.C. §45(a)(1).

6. In addition to sharing the data without consent, Premom allegedly did not provide an option for users to opt-out of the data sharing, and Premom's website privacy policy was inconsistent with its mobile application's privacy policy, the former failing to mention that Premom collects user data.

7. Press Release, Fed. Trade Comm'n, Retail Tracking Firm Settles FTC Charges it Misled Consumers About Opt Out Choices (Apr. 23, 2015), https://www.ftc.gov/news-events/press-releases/2015/04/retail-tracking-firm-settles-ftc-charges-it-misled-consumers.