Separate Statement of Commissioner Noah Joshua Phillips

In the Matter of Flo Health, Inc.
Commission File No. 1923133
January 13, 2021

Despite representing that it would not share its users' health details with anyone, Flo Health, Inc. ("Flo") allegedly did so. As charged in the complaint, Flo coded app events, a mechanism by which app developers use third-party analytics to track how users use their apps, with words like "Pregnancy", and then shared them with analytics divisions of third parties including Facebook and Google.[1] I support this complaint and consent, which sends an important message about the care that app developers must take to level with users about how they share user data.

I write to respond to the vision my colleagues articulate about when the Commission should use consumer notice in our data security and privacy enforcement program.

The order that we place on the public record for comment requires Flo to seek deletion of data it improperly shared with third parties; obtain users' affirmative express consent before sharing their health information with third parties; report to the Commission future unauthorized disclosures; obtain an outside assessment of its privacy practices; and provide the following notice to consumers:

> Between June 1, 2016 and February 23, 2019, the company that makes the Flo Period & Ovulation Tracker app sent an identifying number related to you and information about your period and pregnancy to companies that help us measure and analyze trends, usage, and activities on the app, including the analytics divisions of Facebook, Flurry, Fabric, and Google. No information was shared with the social media divisions of these companies. We did not share your name, address, or birthday with anyone at any time.[2]

In championing the consumer notice remedy in their concurring statement, Commissioners Chopra and Slaughter propose that the Commission no longer assess each case on its particular merits when determining when to order consumer notice.[3] Rather, they assert that "the Commission should presumptively seek notice provisions in privacy and data security matters, especially in matters that do not include redress for victims."[4] I disagree with that approach.

---

[1] The Complaint does not challenge the use of third-party analytics services, upon which developers routinely rely. Because Flo Health coded events with names like "R_Pregnancy_Week_Chosen", rather than something generic like "Event 1", the events conveyed health information. The Wall Street Journal reported this conveyance on February 22, 2019, and the next day Flo Health ceased its conduct.

[2] Consent, Exhibit A.

[3] Commissioners Chopra and Slaughter also assert that the "plain language" of the Health Breach Notification Rule covers Flo. I disagree. We have never applied the Rule to a health app such as Flo in the past, in part because the language of the Rule is not so plain. And I do not support announcing such a novel interpretation of the Rule here, in the context of an enforcement action. *See* Joint Statement of Comm'r Chopra and Comm'r Slaughter, *In re Flo Health*, File No. 1923133 (Jan. XX, 2021).

[4] *Id*.

The Commission has used notice requirements to prevent ongoing harm to consumers and to enable them to remediate the effects of harm suffered. To that end, the Commission has required consumer notice in cases where:

- consumers' health or safety is at risk;[5]
- consumers are subject to recurring charges that they may be unaware of;[6]
- consumers have a financial or legal interest that needs to be protected;[7]
- notice is necessary to prevent the ongoing dissemination of deceptive information;[8] or
- consumers on their own would not have been able to discover or determine the illegal behavior and would not know to take remedial action.[9]

Using these guidelines, the Commission has found consumer notice appropriate in some privacy and data security cases as well, such as when there was a need to inform consumers about ongoing data collection and sharing[10] or to correct a deceptive data breach notification.[11] On the data security front, where it can be critical that consumers know that sensitive information has been breached or exposed, a panoply of state breach notification laws require notice to consumers.

When warranted, notice to consumers can be an important tool. But neither the Commission, nor any of the 50 states with data breach notification laws, have taken the position of requiring

---

[5] For example, in *Daniel Chapter One*, No. 9329 (Jan. 25, 2010) https://www.ftc.gov/enforcement/cases-proceedings/082-3085/daniel-chapter-one, the final order required the respondent to notify consumers that the company's cancer treatment claims regarding its dietary supplements were deceptive, and the supplements could actually interfere with cancer treatment.

[6] For example, in the stipulated final order in *FTC v. Lumos Labs, Inc.*, No. 3:16-cv-0001, at 12-13, 22-23 (C.D. Cal. Jan. 8, 2016), the required notices described the FTC's allegations and explained how to cancel service.

[7] In *FTC v. American Financial Benefits Center*, No. 4:18-cv-00806 (N.D. Cal. Feb. 7, 2018), consumers were notified that their recurring payments to the company were not being used to pay off their student loans.

[8] In *FTC v. Applied Food Sciences, Inc.*, No. 1:14-cv-00851 at 12, 21 (W.D. Tex. Sept. 10, 2014), a wholesaler of dietary supplement ingredients distributed misleading information to supplement makers, touting the results of a clinical study that the FTC's investigation had shown to be botched. The company was required to notify all supplement makers who had received the misleading information that the FTC did not find the study credible.

[9] For example, in *Oracle Corp.,* No. C-4571 (Mar. 29, 2016), https://www.ftc.gov/enforcement/cases-proceedings/132-3115/oracle-corporation-matter, the settlement required Oracle to notify consumers about certain data security risks and explain how to protect their personal information by deleting older versions of Java.

[10] *Unrollme Inc.*, No. C-4692 (Dec. 17, 2019), https://www.ftc.gov/enforcement/cases-proceedings/172-3139/unrollme-inc-matter.

[11] *Skymed International, Inc.,* File No. 1923140 (Dec. 16, 2020), https://www.ftc.gov/enforcement/cases-proceedings/1923140/skymed-international-inc-matter.

consumer notice for the mere sake of the notice itself. Commissioners Chopra and Slaughter stress that notice is warranted especially where redress is not paid to consumers. How consumer notice substitutes for redress, an equitable mechanism to return to consumers what they have lost, is not clear. Nor is it clear what, if anything, limits this approach to notice to data security and privacy cases. To the extent notice is intended as a penalty, I disagree. My view is that we should target notice as a means to help consumers take action to protect themselves. Contacting consumers when there is no remedial action that they can take runs the risk of undermining consumer trust and needlessly overwhelming consumers.[12]

[12] I am also concerned about the possibility of notice fatigue. For example, in the context of security warnings on mobile devices, there is evidence of a decreased neurological response after repeated exposure to warnings. *See, e.g.*, Anthony Vance et al., *Tuning Out Security Warnings: A Longitudinal Examination of Habituation Through fMRI, Eye Tracking, and Field Experiments*, 42 MIS Quarterly, No. 2, June 2018, at 1, https://misq.org/skin/frontend/default/misq/pdf/appendices/2018/V42I1Appendices/14124_RA_VanceJenkins.pdf.