UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of Commissioner
Noah Joshua Phillips

Dissenting Statement of Commissioner Noah Joshua Phillips

Regarding the Policy Statement on Breaches by Health Apps and Other Connected Devices

September 15, 2021

Today a majority of the Commission issues a policy statement to "offer guidance on the scope of the FTC's Health Breach Notification Rule" (the "Statement"). The Statement end runs not one but two ongoing rulemaking processes and relies on a convoluted statutory interpretation to apply civil penalties to a broad swath of conduct never contemplated by Congress. I dissent.

The first problem with the Statement is that it is being issued in the midst of an ongoing rulemaking that considers the very question the statement purports to answer, *i.e.*, whether the Health Breach Notification Rule (HBNR) does and should apply to health-related apps.[1] The Commission has not completed that process, which includes reviewing the comments we have solicited from the public. Declaring the answer ahead of time makes a mockery of the Administrative Procedure Act, which members of the majority have previously touted as nothing less than a solemn exercise in democratic decision-making.[2]

The Statement also ignores a parallel rulemaking process that the Department of Health and Human Services (HHS) has initiated to consider how to define and treat mobile health applications under its HIPAA Privacy Rule.[3] The majority has failed even to consider that rulemaking and its implications in reaching their own decision. This is not how the administrative policy-making process is supposed to work.

---

[1] Health Breach Notification, Request for Public Comment, 85 Fed. Reg. 31085 (Apr. 22, 2020).

[2] Rohit Chopra & Lina M. Khan, *The Case for "Unfair Methods of Competition" Rulemaking*, 87 U. CHI. L. REV. 357, 369 (2020); Keynote Remarks of Acting Chairwoman Rebecca Kelly Slaughter, Consumer Fed'n Of America's Virtual Consumer Assembly (May 4, 2021), https://www.ftc.gov/system/files/documents/public_statements/1589607/keynote-remarks-acting-chairwoman-rebecca-kelly-slaughte-cfa-virtual-consumer-assembly.pdf. This conduct is, regrettably, part of a newly-recurring pattern. The majority, in public meetings and elsewhere, talk the talk of transparency, inclusivity, and public input but walk the walk of refusing to seek input, giving the least notice possible about its plans, and, here, affirmatively end-running a process that might accomplish its professed values.

[3] Proposed Modifications to the HIPAA Privacy Rule To Support, and Remove Barriers to, Coordinated Care and Individual Engagement, Notice of Proposed Rulemaking, 86 Fed. Reg. 6446 (Jan. 21, 2021); Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement, Extension of Comment Period, 86 Fed. Reg. 13683 (Mar. 10, 2021).

The majority surely believe the result they adopt is what consumers of health apps want and need. But the right way to go about it is to conclude the *ongoing* rulemaking process, especially when the statutory and regulatory interpretation on which the majority rely is far from clear.

About the statute and regulations. To arrive at the result in the Statement—*i.e.*, that the HBNR is in fact a broad privacy rule that extends far beyond the personal health record vendors contemplated by Congress—the majority rely on a Rube Goldberg interpretation that is anything but evident. Only eight months ago, in January of this year, a different majority of the Commission did not include a Health Breach Notification Rule count against Flo Health, despite the arguments put forward by two Commissioners.[4] Business education that the agency *has published on our website and that remains there today* conflicts directly with the position the Statement takes.[5] That collection of experience is one important reason why the FTC in May 2020 published a Federal Register notice and requested that stakeholders weigh in on this and other related issues. But never mind all that: three commissioners now consider this settled law.

Their reading of the relevant texts is convoluted, and apparently beyond what Congress, the Commission, and sister agencies had in mind in drafting them. Under it, all applications consumers use to store and process data about anything related to health—*e.g.*, your steps, the food you eat, etc.—are "health care providers". So too would be retailers that sell health care supplies, like Neosporin and vitamins. That broad definition is not the one used by HHS and the Social Security Administration (SSA): those agencies focus on traditional healthcare providers, like doctors, nursing homes, and pharmacies.[6] It also goes far beyond discussion both in Congress and at the Commission at the time the law was written and the HBNR was drafted.[7]

The HBNR requires notifications to consumers of breaches. That is a sensible remedy when, say, a hacker breaches a vendor of personal health records. But a notification obligation is an odd

---

[4] *Cf.* Statement of Comm'r Phillips, In re Flo Health, File No. 1923133 (Jan. 13, 2021).

[5] The majority's view of the definition of a PHR-related entity covered by the HBNR maintaining personal health records that "can be drawn from multiple sources," is out of alignment with business guidance that states:

> If consumers can simply input their own information on your site in a way that doesn't interact with personal health records offered by a vendor – for example, if your site just allows consumers to input their weight each week to track their fitness goals – you're not a PHR-related entity.

FTC Business Guidance, *Complying with the FTC's Health Breach Notification Rule*, https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule.

[6] The SSA defines the term health care provider to include "any other person furnishing health care services or supplies." 42 U.S.C. 1320d(3). HHS has consistently referred to health care providers in terms of traditional forms of health care (*e.g.*, physicians, other practitioners, hospitals, health plans, pharmacies, suppliers of durable medical equipment). For example, the Privacy Rule discusses these terms in the context of health care professionals and institutions. 45 C.F.R. Part 160 and Subparts A and E of Part 164. And, in guidance on its website, HHS gives as examples of health care providers: Doctors, Clinics, Psychologists, Dentists, Chiropractors, Nursing Homes, and Pharmacies. *See* https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html.

[7] *See, e.g.,* GINA STEVENS & EDWARD C. LIU, CONG. RSCH. SERV., R40546, THE PRIVACY AND SECURITY PROVISIONS FOR HEALTH INFORMATION IN THE AMERICAN RECOVERY AND REINVESTMENT ACT OF 2009, at 9 (2009) (listing Google Health and Microsoft HealthVault as examples of PHR vendors). *See also* Health Breach Notification Rule; Final Rule, 74 Fed. Reg. 42962 (Aug. 25, 2009) (preamble of HNBR, discussing PHR vendors that primarily focus on entities managing patient records created by insurers or healthcare providers).

way to police misrepresentations related to privacy. For instance, in the Statement's example of breach by unscrupulous sharing, when does "the discovery of a breach of security" that triggers notification obligations occur? Is it when the vendor "discovers" their own plan to share the data, or comes up with it in the first place, before any information is acquired? Or is it only after that information is shared? Privacy regulations often deal with first-party violations such as these by barring the sharing and penalizing it, thus preventing the violations from happening.[8] Waiting for an ill-defined discovery to occur and then requiring only notification permits the information sharing to happen.

The Statement also goes beyond the text of the statute. It includes as breaches "[i]ncidents of unauthorized *access*, including sharing of covered information without an individual's authorization."[9] But the law limits HBNR to "breach of *security*" defined only as "*acquisition* of such information without the authorization of the individual."[10] That difference matters. The statutory definition of breach for the HBNR differs from the definition of breach for protected health information in other parts of the same statute, which covers "unauthorized *acquisition, access*, use, or disclosure of protected health information which compromises the *security or privacy* of such information."[11] To arrive at its desired outcome, the Statement ignores the distinction drawn by the law itself.

The scope of the Health Breach Notification Rule—and in particular the definitions in our regulations and those of HHS and SSA that the majority is today reimagining—has never been a model of clarity. Government officials and stakeholders alike have wrestled with it. And dramatic revision may have a profound impact in a rapidly-developing area of technology and healthcare. All of that calls for public notice and comment, and a careful consideration of the information the Commission gathers. That is the opposite of what the Commission does today.

[8] *See e.g.*, Health Insurance Portability and Accountability Act of 1996 § 1177, 42 U.S.C. § 1320d-6 (providing criminal penalty for wrongful disclosure of information under HIPAA); Children's Online Privacy Protection Act, 15 U.S.C. 6501-6505, and Rule, 16 C.F.R. Part 312.

[9] Fed. Trade Comm'n, Policy Statement on Breaches by Health Apps and Other Connected Devices (Sept. 15, 2021).

[10] 42 U.S.C. § 17937(f)(1) (emphasis added).

[11] *Id.* § 17921(1)(a) (emphasis added).