UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of Commissioner
Rohit Chopra

PREPARED REMARKS OF COMMISSIONER ROHIT CHOPRA

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

September 15, 2021

When Congress passes a law to punish abuse and misuse of personal data, the Federal Trade Commission should faithfully enforce it. But there are too many examples where Congress has armed the FTC with specific authority to protect this data and our predecessors on the Commission, on a bipartisan basis, chose to do almost nothing at all.

For example, in 2005, President George W. Bush signed legislation authorizing the FTC to codify energy privacy rules, given the rise of a "smart grid" and the resulting risks to both privacy and our national security. In 2017, the U.S. Department of Energy even warned of "imminent danger" of attacks on our grid, and highlighted the "national security and economic vulnerabilities associated with interconnectedness and the growing proliferation of unhardened consumer devices."[1] However, Commissioners serving before us didn't even bother to solicit comment on whether and how to use this tool.

This is just one of many examples where Commissioners have decided that our statutory responsibilities are optional -- a concept we should all find deeply inappropriate.

In 2009, Congress authorized the FTC to finalize a health breach notification rule to protect the public against more digitized personal health data. This would complement some of the protections in the Health Insurance Portability and Accountability Act, or HIPAA. The public would get notice of unauthorized disclosures of their health information and violators would be subject to stiff penalties. The protections were not simply intended to protect the public when a company was hacked. They also sought to deter unauthorized sharing. Fortunately, Congress put in place a deadline for the rule to be put in place, so Commissioners couldn't easily wiggle out of it.

Since February 2010, when the rule took full effect requiring notification for unauthorized disclosures of covered information, the FTC and the public have been notified exactly four times about breaches. Four times. It is impossible that there have been only four covered incidents in our country during this time period. On top of that, the FTC has not collected a single penny in penalties. It is worth underscoring that this covers a period of time when our country experienced a health crisis in which technology became even more central to our healthcare. It is clear that something was not working with our administration of the rule.

---

[1] DEP'T OF ENERGY, TRANSFORMING THE NATION'S ELECTRICITY SECTOR: THE SECOND INSTALLMENT OF THE QER at p. 7-3 (Jan. 2017), https://www.energy.gov/sites/prod/files/2017/01/f34/Chapter%20VII%20A%2021st-Century%20Electricity%20System--Conclusions%20and%20Recommendations_0.pdf.

Last year, Commissioners created more confusion in a law enforcement action against Flo, the popular menstrual tracking app. Flo was improperly sharing extremely sensitive data with Facebook, Google, and others. Rather than sending a clear message that the text of the Health Breach Notification Rule covers a wide range of health and fitness apps, Commissioners demonstrated again that they would not be willing to enforce the law and regulation as written.

But today, the Commission can change course. The Commission previously launched a review to learn more about our Health Breach Notification policies. This was not the launch of a new proposed rule or an advanced notice of proposed rulemaking, but a change for us to learn about what was working and what wasn't. I appreciated the many conversations I had on this topic. The proposed policy guidance is consistent with the existing rule, but more clearly articulates which types of apps and services are covered, given changes in the marketplace when it comes to the collection of health information that is not covered by HIPAA. This is especially useful for the honest businesses not covered by HIPAA seeking to understand their obligations under the law.

I support this effort and I look forward to continuing our work with the Department of Health and Human Services to safeguard our most sensitive health data, and I am pleased we will be taking steps to ensure that data protection laws passed by Congress are faithfully administered and enforced.