FTC Privacy Enforcement Update

Elisa Jillson
Division of Privacy and Identity Protection
Federal Trade Commission

The views expressed are those of the speaker and not necessarily those of the FTC

FTC Background

- Independent law enforcement agency
- Consumer protection and competition mandate
- Privacy and Data Security are consumer protection priorities
  - Enforcement
  - Policy initiatives
  - Consumer education and business outreach

FTC Background

Authority: FTC Act

"**Unfair** or **deceptive** acts of practices in or affecting commerce, are hereby declared unlawful."

Federal Trade Commission Act, Section 5 (15 U.S.C. § 45)

FTC Health Breach Notification Rule

- **Three types of covered entities**
  - Vendors of personal health records (PHRs)
  - PHR related entities
  - Third-party service providers

- **Requires covered entities that suffer a breach to:**
  - Notify everyone whose information was breached
  - In some cases, notify the media
  - Notify the FTC

***Does not apply to entities covered by HIPAA**

HIPAA and the FTC Act

- Section 5 authority extends to both HIPAA and non-HIPAA covered entities
- Sharing Consumer Health Information? Look to HIPAA and the FTC Act (2016)

FTC CONSUMER PRIVACY CASES

Cases Involving Consumer Health Data

- **Henry Schein**
  - Alleged that provider of dental office management software misrepresented industry-standard encryption of patient info
- **Practice Fusion**
  - Alleged that EHR provider misled consumers by failing to disclose adequately that physician reviews would be publicly posted
- **PaymentsMD**
  - Alleged that company and former CEO misled consumers who signed up for online billing portal by failing to adequately inform them that the company would seek highly detailed medical information from pharmacies, medical labs, insurance companies to use for electronic health record portal site

Order Violations and New Section 5 Violations:

- Told consumers that they could limit sharing to groups (e.g., friends) but FB shared the info with app developers.
- Did not adequately assess and address privacy risks posed by third-party app developers.
- Misrepresented that users would have to “turn on” facial recognition technology when, for many, default “on”
- Violated the FTC Act when it told users it would collect phone numbers for security, but did not disclose that numbers used for advertising

As a result:

- $5 billion penalty
- New privacy requirements:
  - Greater oversight of 3rd party app developers (e.g., terminate those that fail to certify compliance with platform policies)
  - Opt-in consent for using/sharing facial recognition info in ways that exceed prior disclosures

Guidance for Mobile Health App Developers

- Interactive tool to help health app developers figure out which federal laws might apply to their app
  - Produced in cooperation with ONC, OCR, and FDA

Produced in cooperation with the U.S. Department of Health & Human Services (HHS): the Office of the National Coordinator for Health Information Technology (ONC), the Office for Civil Rights (OCR), and the Food and Drug Administration (FDA)

The Office of the National Coordinator for Health Information Technology

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

FDA

Guidance for Mobile Health App Developers

- FTC Best Practices
  - Minimize data
  - Limit access and permissions
  - Keep authentication in mind
  - Consider the mobile ecosystem
  - Implement security by design
  - Don’t reinvent the wheel
  - Innovate how you communicate with users
  - Don’t forget about other applicable laws

- Risks to consumer data, especially health apps?
- Third-party transmissions?
- Consumer perception of the privacy and security of products that handle sensitive information?
- Tradeoffs between product functionality and increased security or increased privacy protections?
- Unique attributes or characteristics of health apps?

DNA Test Kits – Consumer Education

- *DNA test kits: Consider the privacy implications* (2018)
  - Comparison shop for privacy
  - Choose your account options carefully
  - Recognize the risks
  - Report your concerns

DNA Test Kits – Business Outreach

- *Selling genetic testing kits? Read on.* (2019)
  - Describe uses of genetic info in one featured place
  - Explain who can see what profile info – and let users know about important changes
  - Help users to make choices with set-wizards and appropriate default settings
  - Explain third-party disclosures clearly
  - Consider one-stop shopping for expunging genetic info

Questions?

Elisa Jillson
Federal Trade Commission
ejillson@ftc.gov