The FTC's Approach to Health Privacy:

Facebook, Health Apps, DNA Test Kits

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

Background

FTC Background

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

FTC Act Fundamentals

- Section 5 of the FTC Act broadly prohibits “unfair or deceptive acts or practices in or affecting commerce.”
  - **Deception**: a material representation or omission that is likely to mislead consumers acting reasonably under the circumstances
  - **Unfairness**: a practice that causes or is likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers

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)

Enforcement

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

Facebook:
Alleged Order 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”

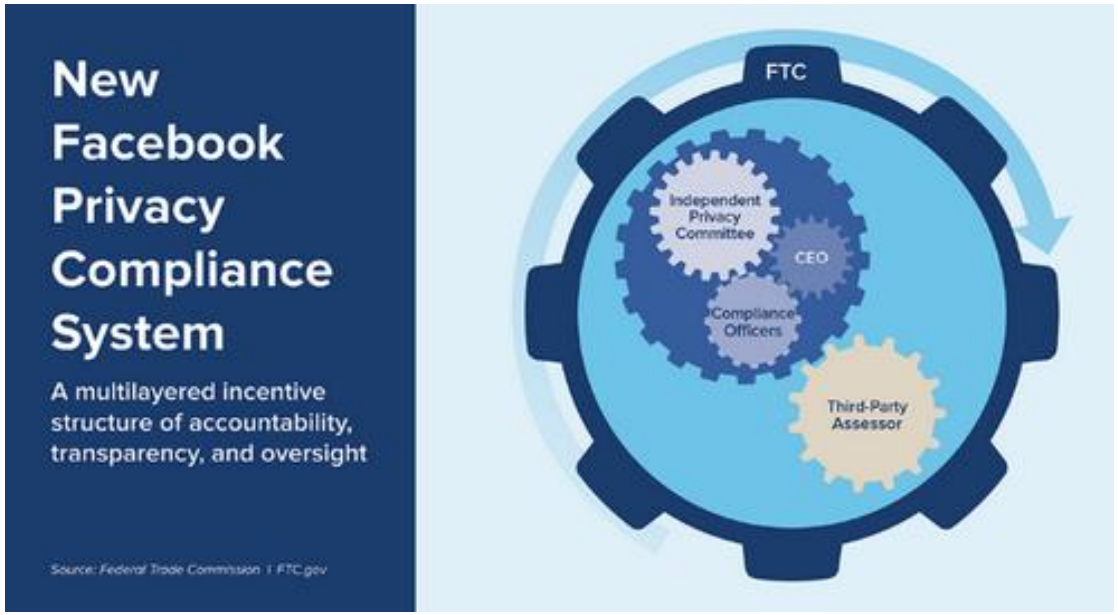
Facebook:
Alleged FTC Act Violation

- Told users it would collect phone numbers for security. Failed to disclose that numbers used for advertising.


FTC Settlement with Facebook
$5,000,000,000
Unprecedented penalty
New privacy structure
at Facebook
New tools for FTC
to monitor Facebook

New Compliance Channels

- Independent Board of Directors focused solely on privacy
- Mark Zuckerberg and Designated Compliance Officers independently certify compliance to FTC
- Independent assessor, whom FTC can fire



Reforms on How Facebook Does Business

- 4 mandatory information flows
  - Must review new or modified product, service, practice and generate what are effectively privacy impact assessments
  - Incident reporting to assessor and FTC
  - Biennial assessment
  - FB management and assessor brief privacy committee quarterly

b. For each new or modified product, service, or practice that presents a material risk to the privacy, confidentiality, or Integrity of the Covered Information (*e.g.*, a completely new product, service, or practice that has not been previously subject to a privacy review; a material change in the sharing of Covered Information with a Facebook-owned affiliate; a modified product, service, or practice that includes a material change in the collection, use, or sharing of Covered Information; a product, service, or practice directed to minors; or a product, service, or practice involving health, financial, biometric, or other similarly sensitive information), producing a written report ("Privacy Review Statement") that describes:

(i) The type(s) of Covered Information that will be collected, and how that Covered Information will be used, retained, and shared;

(ii) The notice provided to Users about, and the mechanism(s), if any, by which Users will consent to, the collection of their Covered Information and the purposes for which such information will be used, retained, or shared by Respondent;

(iii) Any risks to the privacy, confidentiality, or Integrity of the Covered Information;

(iv) The existing safeguards that would control for the identified risks to the privacy, confidentiality, and Integrity of the Covered Information and whether any new safeguards would need to be implemented to control for such risks; and

(v) Any other known safeguards or other procedures that would mitigate the identified risks to the privacy, confidentiality, and Integrity of the Covered Information that were not implemented, such as minimizing the amount or type(s) of Covered Information that is collected, used, and shared; and each reason that those alternates were not implemented;

c. The Designated Compliance Officer(s) shall deliver a quarterly report ("Quarterly Privacy Review Report") to the Principal Executive Officer and to the Assessor that provides: (i) a summary of the Privacy Review Statements generated during the prior fiscal quarter under Part VII.E.2.b, including a detailed discussion of the material risks to the privacy, confidentiality, and Integrity of the Covered Information that were identified and how such risks were addressed; (ii) an appendix with each Privacy Review Statement generated during the prior fiscal quarter under Part VII.E.2.b; and (iii) an appendix that lists all privacy decisions generated during the prior fiscal quarter under Part VII.E.2.a;

Health Apps

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


PRIVACY CON
FEDERAL TRADE COMMISSION
DC // 7.21.20

Background: Greater Use

- Provider and consumer adoption of health apps
  - 93% of physicians think apps can improve health
  - Market projected at $236 billion by 2026
- 21st Century Cures Act
  - New rules expected from ONC and CMS related to patient access
  - Standardized APIs

Background: Potential Risks

- April 2019 research in JAMA on data sharing practices of depression and smoking cessation apps
- March 2019 research in BMJ on data sharing practices of medicine-related apps
- ABC News report: Australian medical appointment-booking app transferred users' personal information to personal injury lawyers

Call for presentations

- 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?

Important Dates

- Research completed after January 1, 2019
- Submission deadline is April 10, 2020
- PrivacyCon is July 21, 2020

DNA Testing Kits

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