Webcast: Understanding and Mitigating the Risks Associated with Online Behavioral Tracking

- September 19, 2023
- Presented by the ACC Health Law Network and Foley & Lardner

Disclaimer:

The views expressed during this program do not constitute legal advice, belong solely to the panelists, and do not reflect the views of the Association of Corporate Counsel or the entities for whom the panelists are employed.

WELCOME AND INTRODUCTIONS

Sean Vargas-Barlow, Moderator

Principal Lead Privacy Counsel, ResMed, Inc.

R. Jason Cronk, Esq.

President, Institute of Operational Privacy Design

Debbie Reynolds, Founder, CEO, and Chief Data Privacy Officer, Debbie Reynolds Consulting, LLC

Aaron Maguregui, Esq.

Senior Counsel, Foley & Lardner LLP

Agenda

- Understanding Issues with Online Behavioral Tracking (“OBT”)
- Assessing the risks of the OBT
- US Privacy Laws Regulating OBT
- What is PbD
- How would you apply PbD to OBT
- Q&A

Why should we care about online behavioral tracking (“OBT”)?

- Emerging Technology: Emerging Technology uses increase OBT privacy and security risks
- Risk Management: Understanding OBT can help in assessing and mitigating associated risks
- Third-party Risks: Understanding OBT helps in evaluating third-party risks and compliance
- Strategic Alignment: OBT must align with the company's cybersecurity and privacy strategy
- Business Reputation: Mishandling OBT can harm a company's image and customer relations
- Ethical Obligations: Responsible OBT upholds the ethical responsibility to protect user information.
- User Trust: Transparent tracking practices are essential for maintaining user trust and reputation

What questions to ask the business in determining what tracking is taking place?

- **<u>Data Privacy and Cyber Security Risk Questions</u>**
  - Privacy by Design: What design considerations can be made to minimize PII data collection and retention?
  - Collection Methods: How is tracking implemented, and what security measures are in place?
  - Consent Compliance: How are users informed, and how is their consent obtained and managed?
  - Security Infrastructure: What cybersecurity measures are in place to safeguard the data?
  - Impact Assessment: How is the impact on privacy and cybersecurity assessed and monitored?
  - Breach Preparedness: What plans and protocols are in place for potential data breaches or violations?

What questions to ask the business in determining what tracking is taking place?

- **<u>Legal and Compliance Risk Questions</u>**
  - Legal Obligations: What are the legal obligations, and how does tracking comply with them?
  - Industry Regulations: Are specific industry regulations affecting tracking, such as healthcare or finance? Are there other regulations like the FTC Breach of Security Rule to be considered?
  - Third-party Evaluation: What third parties have access, and how are they evaluated for security?
  - Data Purpose: Does the data collection and retention align with our stated purpose?
  - Utilization: How is the tracked data used, and does it align with privacy policies?
  - Data Sensitivity: What sensitive information is being tracked, and how is it protected?

Regulatory Timeline

- Timeline
  - January 2021 – FTC Action
  - Critical articles regarding mental health apps and digital health apps
  - Few lawsuits related to tracking technologies
  - June 2022 – Article regarding hospitals use of tracking technologies within calendaring apps
  - August 2022 – Notifications to individuals, OCR, and media regarding technology tracking breaches
  - August 2022 – Filing of multiple class action lawsuits
  - December 2022 – OCR Bulletin: Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates.
  - February/March 2023 – Health Breach Notification Enforcement Action and further FTC Action
  - July 2023 – OCR/FTC Letters

OCR Bulletin

- Published December 1, 2022
- 4 Sections:
  - Defines and explains tracking technologies
  - HIPAA's application to regulated entities use of tracking technologies
  - Tracking on *authenticated* webpages, *unauthenticated* webpages, and mobile apps
  - Guidance to regulated entities when using tracking technologies.

"Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules."

- Dept. of Health & Human Services, Office of Civil Rights, December 1, 2022

Regulatory Implications & Next Steps

- Are tracking technologies being used?
  - Who, what, when, and where?
- Permissible Use?
- Breach Risk Assessment
- What if not PHI? Other federal/state laws may apply.
- Vendor Risk

PRIVACY BY DESIGN

7 Foundational Principles

Sheerprivacy Consulting Group

www.sheerprivacy.com January 1, 2017

The protection of the rights and freedoms of natural persons with regard to the processing of personal data requires that appropriate technical and organizational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features.

#4 Positive Sum, Not Zero Sum

Mirrored windows allow navigation while preventing SURVEILLANCE of cabin activities

#6 Visibility and Transparency

Side's CCTV monitors display all recorded areas to passengers, preventing EXCLUSION risk.

#3 Embedded Into the Design

Hidden fenders and mooring lines DISCLOSURE of side's expensive features.

#5 Life-cycle Protection

Navigation system auto erases GPS parking prior to system shutdown, eliminating SECONDARY USE of boat geolocation data.

#7 Respect for Users

Noise canceling speakers in cabin prevent INVASION of water taxi sounds into sleeping quarters.

#1 Proactive, Not Reactive

Sound proof lavatory prevents EXPOSURE of bodily functions.

#2 Privacy by Default

Main controls in enclosed cabin can be transferred to upward deck if users are not women desire SURVEILLANCE.

Institute of Operational Privacy Design

Design Process Standard

00
Governance Structure

Risk Model

01 IDENTIFY TARGET

02 IDENTIFY REQUIREMENTS

03 TRADE OFF ANALYSIS

04 MANAGE PRIVACY RISKS

05 VERIFY

06 MONITOR

Threat (actors & their means)
Advertisers can target patients based on medical conditions through a mobile App

Vulnerability
Patient are subject to the mobile App's data collection

Adverse consequences
Surveillance, aggregation, and intrusion

Likelihood
Number of patients & the probability that they will surveil the patients, aggregate data and use that data to send targeted advertising

Severity of impact
Survey of social norms around being targeted for medical advertising

Institute of Operational Privacy Design

Design Process Standard

00
Governance Structure

Risk Model

01 IDENTIFY TARGET

02 IDENTIFY REQUIREMENTS

03 TRADE OFF ANALYSIS

Quality Attributes

	Privacy	Profitability	Compliance
Targeted Ads	• Surveillance • Aggregation • Intrusion	• Revenue from Ads • Low cost implementation	• Risk of compliance with data protection laws and regulations
Contextual Ads	• Intrusion	• Revenue from Ads • Higher cost implementation that Targeted	• Lower risk of compliance with data protection laws and regulations
No Ads	• No issues	• No revenue • No costs	• No risk of compliance with data protection laws and regulations

Institute of Operational Privacy Design

Design Process Standard

00

Governance Structure

Risk Model

Likelihood Opportunity Motivation

Number of patients & the probability that they will surveil the patients, aggregate data and use that data to send targeted advertising

Severity of impact Severity

Survey of social norms around being targeted for medical advertising

01 IDENTIFY TARGET

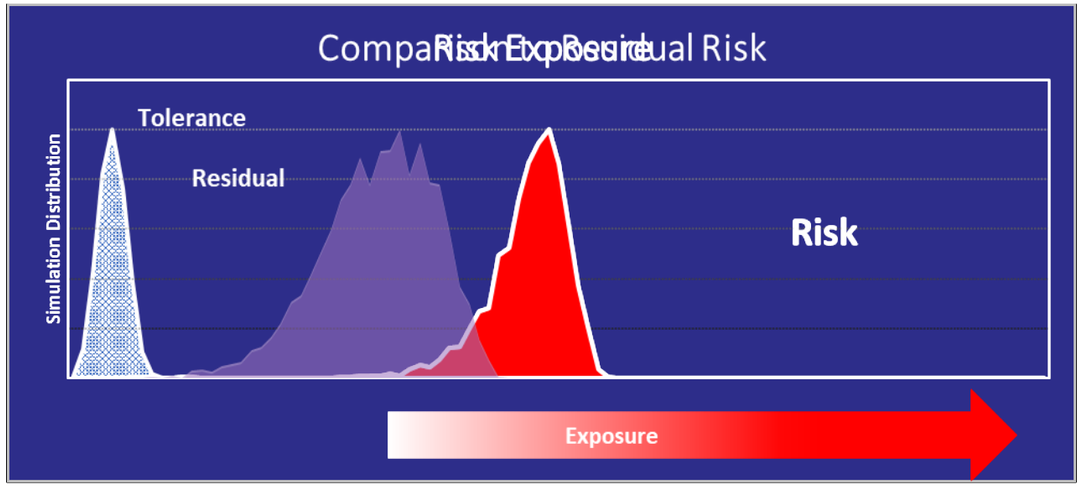
02 IDENTIFY REQUIREMENTS

03 TRADE OFF ANALYSIS

04 MANAGE PRIVACY RISKS

Assess & Respond

Contextual Ads ⇒ *Intrusion*



Institute of Operational Privacy Design

Design Process Standard

00
Governance Structure

Risk Model

01 IDENTIFY TARGET

02 IDENTIFY REQUIREMENTS

03 TRADE OFF ANALYSIS

04 MANAGE PRIVACY RISKS

Assess & Respond

PRIVACY DESIGN STRATEGIES

Opportunity → MINIMIZE & SEPARATE

Motivation → ENFORCE & DEMONSTRATE

Severity → INFORM & CONTROL

Questions

ACC Association of Corporate Counsel

ACC365

ACC how/where/when you want it.

DOWNLOAD TODAY