Trending Privacy Concerns

(in 15 minutes)

Nicholas Merker, CIPT, CISSP

Regulatory Fines

HIPAA Security Rule - Risk Analysis (May 2014)

- “The breach was caused when a physician attempted to deactivate a personally-owned computer server on the network containing patient ePHI. Because of a lack of technical safeguards, deactivation of the server resulted in ePHI being accessible on internet search engines.”
- “Neither entity had conducted an accurate and thorough risk analysis that identified all systems that access ePHI. As a result, neither entity had developed an adequate risk management plan that addressed the potential threats and hazards to the security of ePHI.”

Regulatory Fines

HIPAA Security Rule - Risk Analysis

- "The breach was caused when a physician attempted to deactivate a pers[illegible]-owned computer server on the network contain[illegible]ePHI. Because of a lack of technical safeguard[illegible]tion of the server resulted in ePHI being accessible [illegible]search engines."
- "Neither entity had conducte[illegible]ate and thorough risk analysis that identified all syste[illegible]cess ePHI. As a result, neither entity had developed [illegible]dequate risk management plan that addressed the potential threats and hazards to the security of ePHI."

$4.8 million

Regulatory Fines

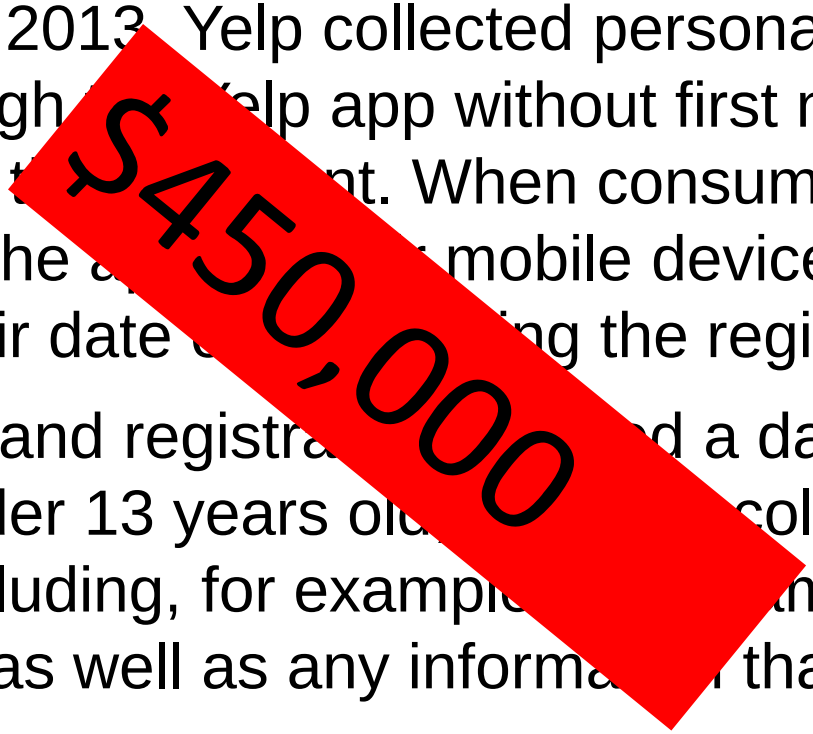
FTC - COPPA

- From 2009 to 2013, Yelp collected personal information from children through the Yelp app without first notifying parents and obtaining their consent. When consumers registered for Yelp through the app on their mobile device they were asked to provide their date of birth during the registration process.
- Several thousand registrants provided a date of birth showing they were under 13 years old, and Yelp collected information from them including, for example, their name, e-mail address, and location, as well as any information that they posted on Yelp.

Regulatory Fines

FTC – COPPA (Sep 2014)

- From 2009 to 2013, Yelp collected personal information from children through the Yelp app without first notifying parents and obtaining their consent. When consumers registered for Yelp through the app on a mobile device they were asked to provide their date of birth during the registration process.
- Several thousand registrants provided a date of birth showing they were under 13 years old, but Yelp collected information from them including, for example, their name, e-mail address, and location, as well as any information that they posted on Yelp.



Regulatory Fines

States (Massachusetts 2011)

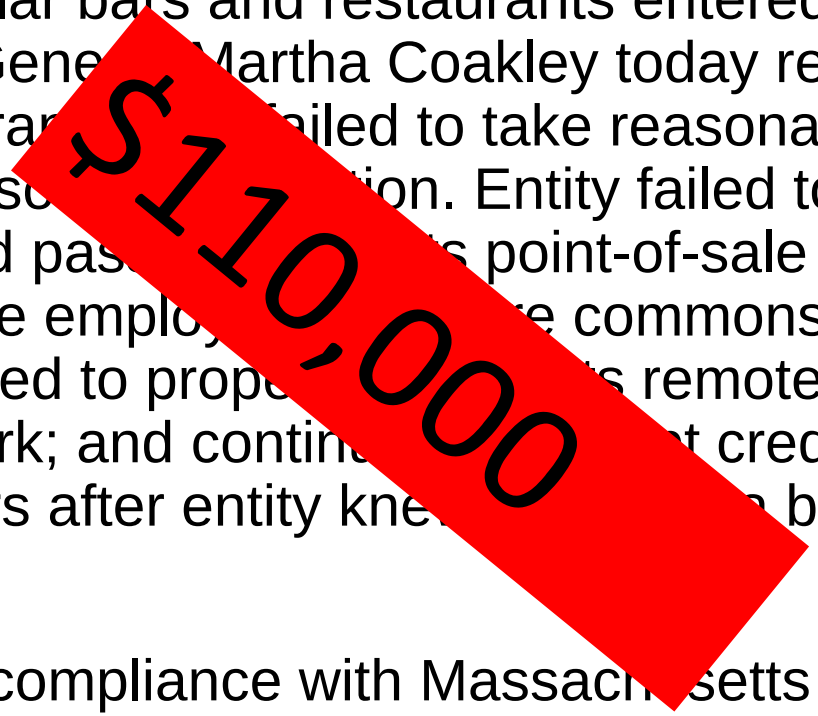
- Owner of popular bars and restaurants entered into a settlement with Attorney General Martha Coakley today resolving allegations that the restaurant chain failed to take reasonable steps to protect its patrons' personal information. Entity failed to change default usernames and passwords on its point-of-sale computer system; allowed multiple employees to share commons usernames and passwords; failed to properly secure its remote access utilities and wireless network; and continued to accept credit and debit cards from consumers after entity knew of the data breach.

- The judgment compliance with Massachusetts data security regulations; compliance with Payment Card Industry Data Security Standards; and the establishment and maintenance of an enhanced computer network security system.

Regulatory Fines

States (Massachusetts 2011)

- Owner of popular bars and restaurants entered into a settlement with Attorney Gene[illegible]Martha Coakley today resolving allegations that the restaurar[illegible]ailed to take reasonable steps to protect its patrons' perso[illegible]ion. Entity failed to change default usernames and pas[illegible]s point-of-sale computer system; allowed multiple emplo[illegible]e commons usernames and passwords; failed to prope[illegible]s remote access utilities and wireless network; and contin[illegible]t credit and debit cards from consumers after entity kne[illegible]breach.



- The judgment compliance with Massach[illegible]setts data security regulations; compliance with Payment Card Industry Data Security Standards; and the establishment and maintenance of an enhanced computer network security system.

Regulatory Fines

North American Electric Reliability Corporation

- 2009-2013:
  - $150 million in fines assessed
  - Largest Settlement: $950,000 (Dec. 2012)

What Do We Do?

- Prevalence and Rigor of Audits Increasing
  - Reevaluate Your Compliance Program
  - Utilize Independent Auditors
  - Utilize Internal Audit Teams
    - Change the Internal Audit Culture

Bring Your Own Device

Bring Your Own Device

Bring Your Own Device

- Preservation for Discovery
- Monitoring
  - Acceptable Use
  - Geolocation
- Security Controls
  - Encryption
  - PIN
  - Remote Wipe

Common Privacy Mistakes

- ***Monitoring***
  - Discovering Information You Do Not Want to Know
  - Using Personal Device Activity in Adverse Employment Decisions
  - Secondary Uses of Collected Information

Common Privacy Mistakes

- ***Security Controls***
  - Remote Wiping Your Employee's Personal Photos and Videos
  - Bricking a Device
  - Banning Applications Important to Personal Use of a Device
  - Failing to Consider Your Compliance Regime for Personal Devices

Privacy Solutions

- BYOD Policy
- Employee BYOD Riders
- Mobile Device Management / Thin Clients
- ActiveSync
- Approved Device Types