PRIVACY LAW 101

Rick Jeffries, CIPP/US

CLINE WILLIAMS WRIGHT JOHNSON & OLDFATHER, L.L.P.

Presented to ARMA May 16, 2018

CLINE WILLIAMS

DISCLAIMER

- I am a lawyer.
- Unless you pay me, and we talk privately, I am not your lawyer.
- This is not legal advice.

- Do not expose to open flame
- Tumble dry low
- Do not remove tag under penalty of law
- Your mileage may vary
- Results not typical

PRIVACY VS. SECURITY

PRIVACY:

Doing the right things with data you obtain.

SECURITY:

Making sure that only the right people access and modify data.

Privacy requires security.

Security does not ensure privacy.

UNITED STATES VS. THE WORLD

UNITED STATES

- Freedom is more important than privacy
- People can collect whatever data they want
- Use of data is restricted by law
- If not restricted, use is acceptable.
- “Opting out” must be honored.

MOST OTHER PLACES

- Privacy is a human right
- Collection and use of data is permitted by law
- If not permitted, collection and use is prohibited
- ”Opt-in” model of consent

GENERAL CONCEPTS

- “Name Plus”: In the US, usually two pieces of data make for identification
- Privacy law does not apply to anonymized data, unless identity of person can be inferred
- Judicial process and litigation are often exceptions to every rule
- Encryption is almost always an antidote
- Security policies and incident plans will usually mitigate punishment from government

GRAMM-LEACH-BLILEY

- Applies to: “Financial Institutions.”
  - Includes: Car dealerships, insurance companies, check cashers, and banks.
- Governs use of “nonpublic personal information” about “consumers”
- Requires:
  - Security for data
    - Training, oversight, technology, locks, plan, responsible person
  - Notice of practices
  - Right to opt out of some sharing

HIPAA

- Applies to:
  - Health care providers ("Covered Entities")
  - Anybody who processes protected health information (PHI) for Covered Entities
- Governs: PHI
- Requires:
  - Privacy notices
  - Business Associate Agreements
  - Authorizations, minimum necessary disclosure
  - Safeguards and accountability
  - Breach notification
- DOES NOT REQUIRE: FAXING

FERPA

- Applies to: Educational institutions that receive federal funds
- Governs: “Education records” – broadly defined
- Requires:
  - Regular notice
  - Nondisclosure
  - Right of access and correction

COPPA

- Applies to: Web site operators and mobile app providers
- Governs: Data collected from children under 13
- Requires:
  - Nondisclosure
  - Verifiable parental consent
- Can affect:
  - Websites appealing to children (toy stores, etc.)
  - Kids apps and games
- Fact-sensitive analysis
  - Primary colors and cute characters

DECEPTIVE TRADE PRACTICES

- State Deceptive Trade Practices Acts/Federal Trade Commission
- Applies to: All commerce
- Governs: False or misleading statements
- Example: Uber
  - We use industry standard practices
  - Engineer posted AWS key to Github
  - Uber paid $100,000 in hush money to hackers.
- You have to do what you say in your privacy policy.
- Note: California law requires every site to have a privacy policy.

STATE DATA BREACH NOTIFICATION LAWS

- Applies to: Unauthorized access to electronic identification
- Governs: Conduct of persons in control of personal data
- Requires immediate analysis after data breach
  - If significant probability of misuse, must notify every affected person
  - Most states require notice to attorney general.
  - Residence of data subject, not location of breached company, controls
- Example: The nice lady who keeps the books

GENERAL DATA PROTECTION REGULATION

- Applies to: Single-piece data about residents of European Union
- Governs: Everything
- Requires:
  - Almost the opposite of every practice acceptable in the US
  - Notifications of subject's rights.
    - Access
    - Rectification
    - Deletion
  - Evidence of consent to contact
  - Minimization
  - Pseudonymization
- GAME. CHANGER.

A GDPR "JOKE"

Q. Do you know of an expert in the GDPR?

A. Yes.

Q. Can you give me her email address?

A. No.

QUESTIONS?

Twitter: @JeffriesInfoSec

rickjeffries@clinewilliams.com

CLINE WILLIAMS