Cybersecurity liability in the US: trends and perspectives

Stacey Dogan
Boston University School of Law
BU Cyber Security, Law, and Society Alliance

Boston University School of Law

Rafik B. Hariri Institute for Computing and Computational Science & Engineering

Overview

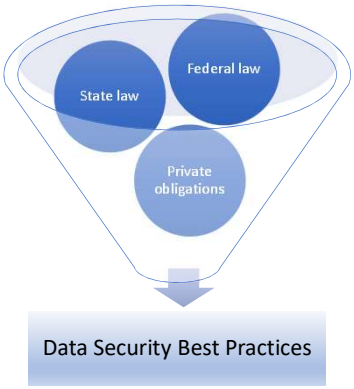
- Regulatory landscape
- Content of rules and obligations
- Hot topics and trends

The regulatory landscape

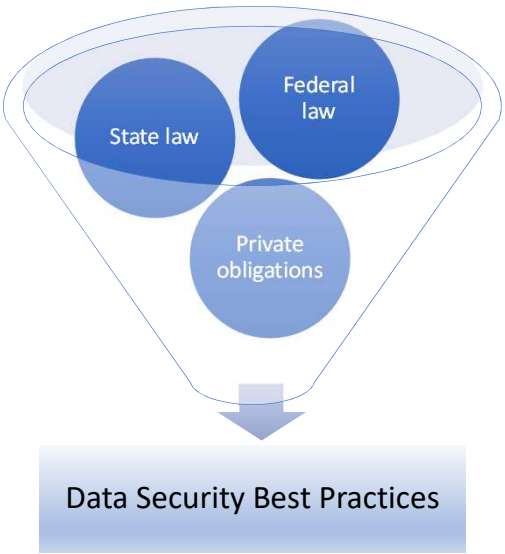
EU

GDPR

US



Sources of Data Security Obligations



Federal Law:
- FTC Act
- Sector-Specific Regulation
- Consent Decrees (FTC, FCC, CFPB, other)

State Law:
- Unfair & Deceptive Acts & Practices Acts (UDAP)
- Data Breach Notification Laws
- Data Security Laws (some sector-specific)
- Private Claims

Private Ordering:
- Voluntary Frameworks/Standards (some sector-specific)
- Certification Authorities
- Contracts

The Substance of Data Security Obligations: Federal Law

General

- FTC Act: Unfair or deceptive trade practices
- Consent Decrees: "Common Law" Best Practices

Sector-specific

- Data-intensive or sensitive industries
  - Health, Education, Finance
- Statutes and agency regulations

The Substance of Data Security Obligations: State Government Enforcement

- Data Breach Notification Laws*
  - All 50 states
  - Must notify consumers and Attorney General
  - Effects:
    - Reputational consequences
    - Risk of enforcement action
    - Result: internalization of costs
- Unfair & Deceptive Acts & Practices Acts (UDAP)
  - State Attorneys General – single lawsuits or multistate actions
    - Settlements: "assurance of voluntary compliance" agreements – best practices
- Specific Data Security Statutes and Formal Guidance (Massachusetts, California)

*precursors to GDPR

The Substance of Data Security Obligations: State Government Enforcement

Commonwealth of Massachusetts v. Equifax (April 3, 2018):

> "The Attorney General, unlike a private litigant … is required only to prove that unfair or deceptive acts or practices took place in trade or commerce; she is not required to prove or quantify resulting economic injury. … She is not required to allege or prove that any individual consumer was actually harmed ….."

The Substance of Data Security Obligations: Private Ordering Trends

- Best practices emerging from consent decrees and AVCs
- Voluntary frameworks/standards (e.g., NIST, CIS Controls)
- Certification authorities (e.g., CISSP) & licensure bodies
- Growing privacy bar; rise of Chief Privacy Officers

Hot Topics and Trends

- Standing
  - *Spokeo, Inc. v. Robins* – concrete injury required for standing
    - Tangible and possible intangible if recognized by law
    - Ongoing uncertainty in lower courts
- Harm
  - FTC: "substantial harm" required for FTC action.
  - States: more flexibility
- Keep Your Eye on the States!
  - Questions about FTC authority (*LabMD*) & political will
  - States as laboratories for progressive change

Keep Your Eye on the States!