Morris, Manning & Martin, LLP

TER | Technology Executives Roundtable

New Privacy Laws

What Tech Companies Must Know – California, New York & International Privacy Law Update

Elizabeth “Bess” Hinson

Bess Hinson, Chair, Cybersecurity and Privacy Practice

- Founder, Atlanta Women in Cybersecurity Roundtable
- J.D., University of Michigan Law School
- M. St., University of Oxford
- B.A., Yale College
- Law Clerk, U.S. Court of Appeals for the Sixth Circuit

- Represents clients at all stages of incident response from investigation, notification, remediation, managing privacy class action risks, and defense of regulatory inquiry
- Cyber and data risk management and governance
- Breach preparedness and table top exercises
- Oversees and coordinates GDPR and CCPA compliance assessment and implementation programs
- Global data privacy compliance
- Internal and external privacy policies
- Employee training programs
- Vendor management
- Data sharing and data monetization agreements
- Strategic advice regarding privacy and data security compliance strategies and programs
- Online advertising and marketing compliance

Shama Barday

OneTrust
Legal Counsel

Sybil Bates McCormack

KeyFactor

In-House Counsel and Director of Contracts

Existing U.S. Privacy Law

- Cable Communications Privacy Act of 1984
- CAN-SPAM Act
- Children's Online Privacy Protection Act (COPPA)
- Consumer Credit Reporting Reform Act
- Drivers Privacy Protection Act (DPPA)
- Electronic Communications Privacy Act (ECPA)
- Electronic Fund Transfer Act
- Electronic Signatures in Global and National Commerce Act
- Fair and Accurate Credit Transactions Act (FACTA)
- Fair Credit Reporting Act (FCRA)
- Family Education Rights and Privacy Act (FERPA)
- Gramm-Leach-Bliley Act (GLBA)
- Financial Services Modernization Act also known Gramm-Leach-Bliley Act (GLBA)
- Freedom of Information Act (FOIA)
- Health Insurance Portability and Accountability Act (HIPAA)
- The Health Information Technology for Economic and Clinical Health Act (HITECH)
- The Privacy Act of 1974
- Telephone Consumer Protection (TCPA)
- Telecommunications Act of 1996
- Telemarketing and Consumer Fraud and Abuse Prevention Act
- Video Privacy Protection Act
- USA Patriot Act

What is Personal Information?

- Ever-evolving definition
- Under the CCPA, eleven categories
- Identifiers, such as:
  - Real name;
  - An alias;
  - Postal address;
  - Email address;
  - Unique personal or online identifier;
  - IP address;
  - Account name;
  - Social Security number;
  - Driver's license or passport number; or
  - Other similar identifiers

What is Personal Information?

- Signature;
- Physical characteristics or description;
- State identification card number;
- Insurance policy number;
- Education;
- Employment or employment history;
- Bank account number, credit card number, debit card number, or any other financial information;
- Medical information or health insurance information
- Products or services purchased, obtained, or considered;
- Biometric information;
- Internet or other electronic network activity information, including:
- Browsing history;
- Information regarding a consumer's interaction with an internet website, application or advertisement.
- Geolocation data
- Professional or employment-related information.
- Inferences drawn from any of these personal information categories to create a profile about a consumer reflecting the consumer's preferences, behaviors, characteristics

California Consumer Privacy Act

- CCPA applies to for-profit entities doing business in the State of California and which satisfy one of the following:
  - annual gross revenues in excess of twenty-five million dollars ($25,000,000) (or the parent meets the $25M threshold);
  - alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or
  - derives 50 percent or more of its annual revenues from selling consumers' personal information.
- Note that to fall under the "at least 50,000 consumers annually" prong, the Company would need only 137 unique California visitors to the website per day, as the definition of personal information includes IP address and device ID.

California Consumer Privacy Act

- Requires businesses to provide consumers with privacy notices and the right to request/access/delete their data
- Creates private right of action relating to data breaches
  - Unauthorized access in violation of duty to maintain “reasonable security”
- Noncompliance penalties of $7,500 or $2,500 per violation

California Consumer Privacy Act

- How will the California Privacy Act (CCPA) impact my tech company?
  - Map data
  - Customer contracts
  - Vendor contracts
  - Privacy disclosures (end users and employees)
  - Timely respond to individual requests

Other New State Privacy Laws

- What other states have privacy laws and how will recent amendments to those laws affect my B2B tech business?
  - New York
  - Nevada
  - Washington State
  - Illinois

New York SHIELD Act

- The Stop Hacks and Improve Electronic Data Security Act (the "SHIELD Act") requires businesses to establish a data security program and prescribes specific components when implementing administrative, technical and physical safeguards.
- Effective March 21, 2020.

New York SHIELD Act

- Covers any business that retains computerized private information of New York residents must develop a data security program to protect the private information.
  - Private information defined as unencrypted information that can identify a person in combination with a social security number, driver's license number, financial account information, including an account number, credit or debit card number, biometric information, a user name or email address in combination with a password or any unsecured protected health information held by a "covered entity."

New York SHIELD Act

- Applies to small businesses
  - A small business is defined as a business with (1) fewer than fifty employees; (2) less than three million dollars in gross annual revenue in each of the previous three fiscal years; or (3) less than five million dollars in year-end total assets
  - Any business defined as a small business under the SHIELD Act is deemed to be compliant with the data security requirements if the small business's security program has reasonable administrative, technical and physical safeguards that are appropriate for the size of the business, the nature and scope of the business's activities, and the sensitivity of the personal information that the business collects from consumers.

Georgia Privacy Laws

- Does Georgia have laws addressing the collection and processing of consumer personal information?
- Are Georgia laws likely to be amended?
  - Ohio Affirmative Defense model

International Privacy Laws

- How will the GDPR and other international privacy laws impact my business?
  - Data Transfer
    - Privacy Shield
    - Other legal transfer mechanisms
  - Notice and Consent
  - Regulatory Authorities

GDPR & Data Breaches

- Became effective May 25, 2018
- Article 33 requires notification to the relevant DPA within 72 hours, where feasible (unless breach is unlikely to result in risk to data subjects)
- Notification must be made if there is a “high risk to data subjects rights and freedoms
- Potential fines up 4% of annual global revenue

Compliance Programs

- What compliance steps and programs should my tech company implement?
  - Incident Response Plan
  - Privacy Policy
  - Privacy Standard
  - Data Retention Policy
  - Data Classification Policy
  - Data Subject Access Request Policy and Procedure
  - Acceptable Use Policy

Leading Your Company Through Incident Response

- Preparation
  - What should my company do to prepare?
  - How expensive is it?
- Response Team
  - Do I need a response team?
  - Who will I need?
- Communication
  - How do I communicate to my company's leadership?
  - How do I communicate to the public?

Third Party Provider Incident Management

- Building a Compliant Third Party Vendor Management Program
  - What must we require of vendors, third party service providers, customers, for purposes of incident response?
  - What are best practices for helping third parties understand their obligations?
  - What are best practices for tracking third party vendor compliance with security incident reporting provisions?
- Increased Cost and Burden of Ensuring Provider Compliance with Contractual Reporting Requirements

Technology Tools for Data Security & Privacy Compliance

- Does technology exist to help with GDPR compliance?
- What technologies exist to assist with other cybersecurity and privacy laws and regulations?

Penalties for Non-Compliance

- Multiple enforcement agencies
- Multi-jurisdictional fines
- Per violation penalties
  - One person = $2,500
- Class action risks
  - Impleaded party if service provider
- GDPR
  - Up to 4 percent gross annual revenue

Cyber Liability Insurance

- Does a cyber liability insurance policy cover the costs related to data breach?
- Does a cyber liability insurance policy cover the costs related to regulatory enforcement actions?
- What is covered under a cyber liability insurance policy?
- How much coverage should my company purchase?

MORRIS, MANNING & MARTIN, LLP

QUESTIONS?