The New Massachusetts Data Breach Law
An Update

Live Webinar

Colin Zick and Christopher Hart
Foley Hoag, LLP

Colin J. Zick

Partner, Chair, Privacy and Data Security Practice

Boston | +1.617.832.1275 | czick@foleyhoag.com

- Serves as Chair of Foley Hoag's Privacy and Data Security practice group. Colin counsels clients ranging from the Fortune 1000 to start-ups on issues involving information privacy and security, including compliance with state, federal and international data privacy and security laws and government enforcement actions. He also frequently counsels technology and consumer-facing clients on issues involving information privacy and security (including the GDPR and Privacy Shield, HIPAA and other U.S. federal and state data privacy and security laws, privacy policies, cloud security, cyber insurance, the Internet of Things, and data breach response).

- Colin co-founded the firm's Privacy and Data Security Practice Group and regularly contributes to its "Security, Privacy and the Law" blog, www.securityprivacyandthelaw.com.

- Colin has been ranked as one of the Best Lawyers in America® since 2015, ranked by CHAMBERS USA as one of Massachusetts' leading health care lawyers since 2010, and he has been selected by his peers as a Massachusetts "Super Lawyer" since 2004. Colin also serves as a member of Law360's Privacy & Consumer Protection editorial advisory board.

Christopher E. Hart

Counsel

Boston | +1.617.832.1232 | chart@foleyhoag.com

- With significant trial litigation, appellate advocacy and cybersecurity experience, has counseled and represented sovereign nations, Fortune 500 companies, start-up companies, non-profits, and individuals in a wide variety of contexts for over a decade.

- Co-chairs the firm's Blockchain and Cryptocurrency practice group. He is also a Certified Information Privacy Professional (CIPP/US, CIPP/E, CIPM), a member of the firm's Data Privacy and Security Group, and a member of the IAPP's Advisory Board (Privacy Bar Section). He has considerable experience in data privacy and cybersecurity issues, and advises companies on regulatory compliance, data breach planning and response, the EU's General Data Protection Regulation (GDPR), and risk management (including cyber insurance).

Agenda

- Data Privacy: The Big Picture of the Legal Landscape
- Data Privacy in Massachusetts: The Rules and How They Have Changed
- Real-World Impacts of the New Massachusetts provisions
- Other Upcoming Changes: GDPR, CCPA, and More
- Takeaways

Data Privacy: The Big Picture of the Legal Landscape

- Privacy versus security: different but complementary concepts.
- No single comprehensive data privacy law for the U.S.
- Federal laws are sector-specific, such as HIPAA for certain types of health data.
- There are as many state data privacy laws as there are states.

Data Privacy: The Big Picture of the Legal Landscape

- There are important consequences to the legal patchwork of state laws:
  - These different privacy laws protect different information and protect it differently.
  - Notification triggers and obligations differ:
    - Consumers and regulators often receive notice
    - But when and how notification is made in the event of a breach can differ significantly.
  - Safe harbors may or may not be provided.

Data Privacy in Massachusetts: The Rules and How They Have Changed

- Massachusetts has a number of different laws touching on privacy, which came about because of the TJX breach.
- The two most important ones for our purposes:
  - M.G.L. c. 93H (statute).
  - 201 CMR 17.00 (regulation).

Data Privacy Obligations in Massachusetts Law

- Chapter 93H
  - What counts as personal information?
  - What counts as a breach?
  - Who do you have to notify?
  - By when?
- 201 Code of Mass. Regulations 17
  - Concerns data security obligations
  - Must take internal steps, train staff, vet third party contractors.

Data Privacy in Massachusetts: How the Rules Have Changed

- Chapter 93H Changes
  - In the event of a breach, consumers must be provided 18 months of free credit monitoring
  - Consumer notification rules have amended:
    - Add person responsible.
    - Inform regulators whether a company has a WISP.
    - Must include name of a parent or affiliated corporation.
    - Cannot delay notification to determine scope of impact.

Data Privacy in Massachusetts

- Equifax litigation
  - 93H was amended in part as a result of the Equifax breach.
  - Case law from the Equifax case has clarified the contours of Chapter 93H in important ways.

Real-World Impacts

- Generally, data privacy laws can place significant obligations on organizations:
  - Policy drafting.
  - Internal auditing.
  - Data breach response.
  - Security protocols.
  - Internal governance.

Real-World Impacts

- Changes to 93H can have significant cost impacts:
  - Requiring credit monitoring for 18 months can be a significant cost consideration.
  - Companies should consider reaching out to credit reporting agencies before a breach to consider contracts.
  - Costs of notification and credit monitoring could suggest revisiting cyber insurance.

Real-World Impacts

- Changes to 93H can have significant impacts on policy drafting and data breach response:
  - Create a WISP if you do not have one.
  - Consider how to best investigate a breach to coincide with more aggressive notification requirements.
  - Must communicate with parent or affiliate who could be named in a breach notification.

GDPR, CCPA, & Upcoming Changes

- Are there other changes in store for Massachusetts?
  - Current draft legislation.
  - GDPR has already changed how companies doing business internationally comply.
  - CCPA, depending on its final form, could signal a shift in the U.S. approach to individual privacy.

Takeaways

- Review internal privacy and security policies.
- Determine your data breach response plan.
- Consider vendor contracts with a credit monitoring agency.
- Consider cyber insurance.
- Be ready for more changes.

Questions?

- Stay up to date by following Foley Hoag's privacy and data security blog, *Security, Privacy, and the Law* - https://www.securityprivacyandthelaw.com/

Save the Dates!

June 14, 2019- 8:00-10:30 am -Best Practices of Sustainability
Wayne Bates- Ph.D., PE., Principal Engineer- Tighe & Bond,
Cristina Mendoza-Solutions Design Lead-Capaccio Environmental Engineering, Inc and
Dr. Mathew Gardner- Founding Director- Sustainserv, Inc.
will discuss the fundamentals of sustainability and how to create value along your sustainability journey.
Location: R.H. White Companies, Auburn MA
Cost: Member Free-Non-Member-$100.00
June 14, 2019-Best Practices of Sustainability

June 19, 2019- 12-1-Brownbag Lunch Webinar- John Regan
Location: One Beacon Street, Boston, MA
Cost: Member Free-Non-Member-$50.00

June 26, 2019- 1-2-Marijuana and its Impact on the workforce
Lori Bourgoin, SVP Field Operations, AIM HR Solutions,
Daniel C. Carr, Associate Attorney at Royal, P.C,
James McMahon, Massachusetts Cannabis Business Association (MassCBA) and
Jay Myers, Public Policy Advisor at Locke Lord LLP
Location: One Beacon Street, Boston, MA
Cost: Member Free-Non-Member-$50.00
June 26, 2019 Webinar-Medical Marijuana in the Workplace