GDPR, CCPA, and All That Jazz

Colin Zick, Esq. and Chris Hart, Esq.
Foley Hoag LLP
September 12, 2019

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.

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).

CCPA: Background

- Consumer Rights Under the CCPA:
  - Right to opt-out of sales of personal information.
  - Right to be forgotten (right to delete).
  - Right to request information about personal information.
  - Antidiscrimination rights.

Note: These rights are qualified.

FOLEY HOAG LLP

CCPA: Application & Effective Date

- Application & Effective Date:
  - Generally applies to for-profit companies that “do business” in California and have revenues > $25m.
  - Covers California Residents’ “personal information.”
    - Defined broadly to cover nearly all information that can be linked to a particular individual, including “cookies” and other online identifiers.
    - Exceptions for certain medical / financial I
    - nformation.
  - January 1, 2020 effective date; likely July 1, 2020 enforcement date.
  - The legislative amendment process is ongoing.
  - Attorney General expected to propose regulations this fall, subject to at least one notice-and-comment period.

FOLEY HOAG LLP

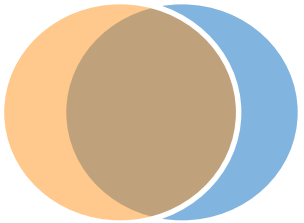
CCPA: Compliance & Liabilities

- Compliance Obligations:
  - Maintain privacy policy that discloses consumer rights, how they can exercise their rights, and what information the company collects/shares.
  - Respond to consumers' requests to exercise their rights.
  - Issue disclaimers regarding collection and use of personal information at or before the point of collection.
- Civil Liabilities:
  - Attorney General: Civil Penalties
  - Private Rights of Action for Security Breaches
    - For breaches of "nonencrypted or nonredacted personal information" caused by a "business's violation of the duty to implement and maintain reasonable security procedures and practices."

FOLEY HOAG LLP

CCPA and GDPR

- General Data Protection Regulation (GDPR)
  - Landmark EU digital privacy legislation
  - Large overlap with approach of CCPA:
    - Right to disclosure and access
    - Right to data deletion
    - Type of information regulated (identifiable to individual)
    - Definition of “personal information”
    - Privacy notice requirement
    - Security measures requirement
    - Extraterritoriality
  - But significant differences:
    - Scope and territorial reach (GDPR is broader)
    - Right to opt-out (GDPR doesn’t provide one)
    - Children’s data (GDPR is more protective)
    - Right to rectification (CCPA doesn’t provide one)
    - Private right of action (GDPR is broader)



FOLEY HOAG LLP

CCPA and HIPAA

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - Federal law protecting certain medical information
  - CCPA exempts
    - Protected Health Information (PHI) (healthcare or healthcare payment information created, received, or transmitted by a HIPAA-covered entity).
    - Personal information that HIPAA-covered entities handle like PHI.
  - Most likely to benefit from this exemption
    - Health care providers
    - Health insurers
  - These companies collect personal information that is **not** exempt
    - Employment information.
    - Electronic network activity information (e.g., cookies).

FOLEY HOAG LLP

CCPA and GLBA

- Gramm-Leach-Bliley Act (GLBA)
  - Federal law protecting certain financial information
  - CCPA exempts
    - Personally identifiable financial information (information a company obtains in connection with providing a financial product or service).
  - Most likely to benefit from this exemption
    - Banks.
    - Financial services companies.
  - These companies collect personal information that is **not** exempt
    - Information collected during marketing process but prior to application for financial product or service.
    - Electronic network activity information (e.g., cookies) not associated with receipt of financial product or service.

GDPR – Recent Enforcement Actions

- Recent matters:
  - British Airways (7/8/19): £183 million by the UK ICO
    - Use of poor security arrangements that resulted in a 2018 web skimming attack affecting 500,000 consumers
  - Marriott International (7/9/19): £99 million by the UK ICO
    - Failure to undertake sufficient due diligence when acquiring Starwood hotels group, whose systems where compromised in 2014, exposing approximately 339 million guest records.
  - Unnamed medical company (8/12/19): €55,000 by the Austrian DSB
    - Not appointing a DPO, not publishing its contact details or reporting those to the supervisory authority, obligatory consent of data subjects (Art. 7), not providing information (Art. 13, 14), no DPIA despite handling sensitive data (Art. 35).

Takeaways from Recent GDPR Activities

- Enforcement is real.
- Enforcement is not uniform.
- Large companies *and* smaller companies – but mostly large companies.
- Compromises are more likely to lead to fines, as opposed to mere non-compliance.
- Many questions remain unanswered.

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 (not privacy) obligations.
  - Must take internal steps, train staff, vet third party contractors.
  - Must memorialize security protocols.

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
  - Notification rules have been amended:
    - Name the person responsible for the breach (if known).
    - 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.

FOLEY HOAG LLP

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.
    - Mere existence of a breach is not itself a violation of Chapter 93H.
    - But awareness of security problems and a failure to fix those problems can raise a claim.
    - So can failure to take reasonable steps to understand threats.
    - Finally, holds that creating and owning a database of consumer information counts as “owning” personal information for purposes of 93H, even if the underlying data belongs to a different entity.

FOLEY HOAG LLP

Other New Laws?

- New York SHIELD Act.
  - Broadens definition of personal information.
  - Breach includes access, not acquisition.
  - WISP
- Nevada
  - Amended its privacy law to allow for opt-out of sale of personal information.
- Massachusetts?
- New WISP laws (usually for insurance industry).
- Changes to FTC rules.
  - Notice and comment for COPPA rules.
  - GLBA Rules
- Federal law?

FOLEY HOAG LLP

Real-World Impacts

- Generally, data privacy laws can place significant obligations on organizations:
  - Policy drafting.
  - Internal auditing.
  - Data breach response.
  - Security protocols.
  - Internal governance.
- Each of these has to be rethought in light of new laws or changes to existing laws.

FOLEY HOAG LLP

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.

FOLEY HOAG LLP

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.
- The CCPA also can have significant impacts:
  - Requires data mapping.
  - Notification obligations can be onerous (e.g., cookies).
  - Opt-out for selling personal data can also be a compliance cost.
- GDPR enforcement activities and additional guidance require diligence.
  - Can affect security protocols, ways of obtaining consent, and contractual obligations.

FOLEY HOAG LLP

Questions?

FOLEY HOAG LLP

Thank you.

Colin Zick

Partner, *Co-Chair, Health Care Practice and Privacy & Data Security Practice*
Foley Hoag LLP

czick@foleyhoag.com | 617.832.1275

Chris Hart

Counsel, Privacy & Data Security Practice
Foley Hoag LLP

chart@foleyhoag.com | 617.832.1232

. . . and read our blog,
www.securityprivacyandthelaw.com