CCPA: What You Need to Know Now and What to Expect in the Future

Colin Zick, Esq. and Chris Hart, Esq.

Foley Hoag LLP

April 28, 2020

Colin J. Zick

Partner, Co-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

Partner, Co-Chair, Privacy and Data Security Practice

Boston | +1.617.832.1232 | chart@foleyhoag.com

- Serves as Chair of Foley Hoag's Privacy and Data Security practice group. 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.

CCPA: Application & Effective Date

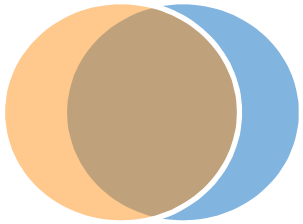
- Application & Effective Date:
  - Generally applies to for-profit companies that “do business” in California and have revenues > $25m.
  - Covers California Residents’ “personal information.”
    - Defined broadly to cover nearly all information that can be linked to a particular individual, including “cookies” and other online identifiers.
    - Exceptions for certain medical / financial information.
  - January 1, 2020 effective date; July 1, 2020 enforcement date.
  - Regulations are nearly final but still being updated.

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."

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)



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).

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.

COVID-19: Compliance Questions

- Different enforcers sending different signals
  - California Attorney General
  - Office for Civil Rights, Health and Human Services
  - Federal Trade Commission
  - EU Member States
- Compliance efforts need to continue
  - But what if the shutdowns have slowed or stopped your compliance efforts?
  - How will you train your staff remotely?

COVID-19: New Privacy and Security Issues

- Privacy and security questions raised by remote work (e.g., Zoom)
- Increase in cyberattacks, ransomware, funds interceptions
- Privacy questions for employers through digital transformation
- New privacy concerns arising from test-and-trace, need for health-related surveillance (e.g., temperature checks, mandatory workplace testing)
- What comes next?
  - Policies for transitioning back from remote work
  - Identifying compliance gaps based on the remote work transition

Other State Law Changes

- New York SHIELD Act
- Proposed legislation in
  - Massachusetts
  - Maryland
  - Hawaii
  - California (!)
- Increasing concerns about biometrics and AI

FOLEY HOAG LLP

Real-World Impacts

- Privacy and security laws can place significant obligations on organizations:
  - Policy drafting.
  - Internal auditing.
  - Data breach response.
  - Security protocols.
  - Internal governance.
- COVID-19 creates a need and opportunity for fresh thinking.

FOLEY HOAG LLP

Questions?

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

Partner, Co-Chair, Privacy & Data Security Practice
Foley Hoag LLP

chart@foleyhoag.com | 617.832.1232

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