Procopio

Latest Developments in Privacy Law

How Companies Should Navigate Increasing Privacy and Cybersecurity Complexity

June 8, 2023 – Session 2

Elaine F. Harwell, CIPP/US, CIPM
Partner, Procopio
Elaine.Harwell@Procopio.com
619.906.5780

Nick Ginger, FIP, CIPP/US, CIPP/E, CIPM
Senior Vice President and Senior Counsel
City National Bank
Nick.Ginger@cnb.com
619.889.6851

Overview of Discussion

- Where are we today? General overview of privacy laws
- Meeting privacy obligations
- Developing flexible privacy program
- Data security programs, illustrated by review of recent FTC cybersecurity enforcement actions
- Questions?

Procopio

Data Privacy Laws:
Where are we today?

- Data privacy laws can broadly impact all businesses
- No single omnibus data privacy law in the U.S. (still)
  - Federal statutes primarily sector-specific; state statutes more focused on rights of individual consumers
- California's focus on consumer privacy
  - First state to pass a comprehensive consumer data privacy law, the California Consumer Privacy Act of 2018 (CCPA)
  - November 2020, California voters voted to amend the CCPA, the California Privacy Rights Act (CPRA)
- Other states have since followed CA with their own comprehensive consumer data privacy laws (VA, CO, CT, UT, IN, IA, TN, MT), more being contemplated
- Federal data privacy law? Not yet, but: American Data Privacy and Protection Act?

California Focus:
California Consumer Privacy Act (CCPA)

- The CCPA (now in effect with amendments)
  - Consumer Rights: to know, delete, correct, opt-out of sale/sharing, non-discrimination
  - New Business Obligations: notices to consumers/employees/B2B contacts, limitations on data "sales" and "sharing" for cross-context behavioral advertising
  - Enforcement (of amendments and newly adopted regulations) begins 7/1/23
- Threshold application to the law:
  - $25MM annual gross revenue; or
  - Collection of 100,000 or more residents' PI; or
  - 50% of annual revenue from sale of PI

Meeting Privacy Obligations:
How do you do it?

- Importance of a privacy program and “team”
  - Privacy Champions
  - Integration of Legal, Info Sec (IT), Compliance
- Focus on the privacy principals
  - Understanding the exemptions in privacy laws
  - Understanding what your website does
- Be on the lookout for emerging issues
  - Children’s data
  - Biometric laws
  - Federal privacy law

Developing a Privacy Program:
Key drivers

- Preliminary considerations:
  - Data governance
  - Globalization
  - Increased regulations
  - Growth of vendor networks
  - Increased sensitivity
- Operational considerations:
  - Industry and business
  - Types of data (and personal information) collected
  - Geographic footprint

Developing a Privacy Program:
Core privacy program functions

- Thought leadership & strategy
  - Privacy compliance is an ongoing concern
  - The need for flexibility
- Cross-functional support within the business
  - Integration among the teams
- Understanding the risks
  - Threats to the business / data
  - Vulnerabilities
  - Likelihood of threats occurring
  - Harm to the business if the threats occurred
  - Reputational risks
- Supporting business operations
  - Working with product developers
  - Working with HR
  - Addressing issues that arise as the company markets and sells products/services

Developing a Privacy Program:
Understanding legal requirements

- Determining applicable laws
  - Type of information collected
  - Jurisdictions
  - How data is used
- Regulated Industries
- Other federal or state guidance
  - White House Executive Orders
  - NIST
  - Guidance from state attorneys general (especially California)
  - International Organization for Standardization (ISO) standards
  - FTC consent decrees, complaints, case summaries

Developing a Privacy Program:
Policies and internal controls

- External privacy statements
  - Website privacy policies
  - Mobile App privacy policies
  - Privacy statements and policies for products/services
  - Just-in-time or notices at collection
- Internal privacy policies and procedures
  - Employee data
  - Employee-facing
  - Incident and security breaches (IRPs, reporting and tracking)
  - Acceptable use policies (newest one: generative AI)
  - Record retention and disposal policies
  - Vendor / third-party privacy requirements

Developing a Privacy Program:
Addressing ongoing compliance

- Providing privacy training and awareness programs
  - Key component that may be required under some laws (e.g., HIPAA)
- Monitoring and auditing compliance efforts
  - Identify compliance gaps
  - Verify internal controls and policies are being followed
- Evaluating and revising program controls, policies, and protocols
  - Are there new threats or risks? Are existing controls adequate?
  - What changes to the law impact the business?
  - What is the industry doing?

Data Security:
Federal Trade Commission

- Why the Federal Trade Commission (FTC)?
  - Primary federal data security regulator in the U.S. for last 20 years
  - Numerous data security enforcement actions under Section 5 of the FTC Act for unfair or deceptive trade practices
  - Section 5 applies to most companies and individuals doing business in U.S. other than certain transportation, telecommunications, and financial companies regulated by other federal agencies
- FTC Act grants rulemaking and enforcement authority under Section 5, but FTC has not enacted rules or regulations that apply to data security requirements
  - August 2022 – FTC issued an Advance Notice of Proposed Rulemaking on Commercial Surveillance and Data Security
- What to do until then?
  - FTC publishes guidance and brings enforcement actions in both privacy and data security contexts
  - Data security complaints; consent decrees
  - (Some) case law

Data Security:
Lessons from FTC Enforcement Actions

- Section 5 provides authority to FTC to protect consumers from unfair or deceptive trade practices in or affecting commerce
- FTC has challenged inadequate security practices as unfair and in some cases as deceptive
- FTC uses privacy policy as basis for enforcement actions
- Common enforcement methods:
  - Administrative process, cease-and-desist orders, generally resulting in consent decrees
  - Complaints in court seeking injunction and consumer redress against defendants

Data Security:
FTC Data Security Guidance

- FTC complaints have become more specific following challenges to their authority and allegedly vague data security standards
- FTC complaints can be guidance for the types of data security practices to implement or avoid
- Regular enforcement actions against organizations that suffer data breaches
  - These enforcement actions frequently allege misrepresentation and unfair practices based on claims that the business failed to provide reasonable and appropriate security

Data Security:

Examples of inadequate security allegations

Business created unnecessary risks to personal information by:

- storing sensitive information on portable media or transporting portable media containing personal information in a manner that made it vulnerable to theft;
- failing to adequately supervise a service provider's collection, use, and retention of personal information;
- failing to take reasonable steps to render backup tapes and portable media unreadable;
- failing to adequately restrict access to or copying of personal information;
- failing to destroy personal information when there was no longer a business need to retain it;
- using outdated and cryptographically broken hashing functions to store passwords;
- storing information in unencrypted files.

Data Security:

More examples of inadequate security measures

FTC complaints alleging failures to:

- adequately train employees on data security measures;
- use reasonable measures to enforce security policy compliance;
- employ sufficient measures to prevent, detect, or investigate unauthorized access to or attacks on computer networks, websites, cloud services, or other resources that store sensitive information;
- implement low-cost technologies that reduce the risk of data breaches;
- reasonably limit administrative control of an organization's systems or data;
- require network administrators and others to use phishing-resistant multifactor authentication or, under earlier actions, strong passwords or different passwords to access different programs, computers, and networks;
- support secure product or service development practices;
- adequately assess risks to consumer information.

Data Security:

Misrepresentations regarding data security practices

- FTC complaints often allege that an organization acted deceptively or unfairly by both:
  - Making implicit or explicit promises about protecting sensitive information.
  - Failing to abide by those promises because of inadequate data security measures.
- FTC often relies on an organization's failure to follow promises contained:
  - Privacy policies;
  - Statements on websites;
  - Marketing information; and
  - Other consumer communications (oral communications, FAQs, publications, etc.)

Data Security:
Examples of misrepresentations

A Company's failure to:

- Implement reasonable policies and practices to protect consumers' personal information.
- Employ reasonable measures to detect and prevent unauthorized access to personal information, including not:
  - performing basic security checks;
  - implementing low-cost security measures; or
  - having adequate processes in place for receiving vulnerability reports from third parties and acting on them.
- Implement policies and procedures to properly dispose of sensitive information, including failing to train employees on proper disposal.
- Prevent unauthorized access to nonpublic user information.
- Honor consumers' privacy choices.
- Use reasonable measures to assess or ensure employee compliance with policies and procedures, for example, by failing to implement training and oversight programs.
- Maintain adequate multifactor authentication or password security.
- Implement or enforce policies sufficient to secure administrative access.
- Require service providers to employ appropriate safeguards for personal information shared with them.
- Reasonably oversee service providers' data security practices.
- Use readily available network and cloud services security measures.
- Delete personal information on a network when there is no longer a business need
- Truthfully disclose status of encryption for sensitive info

Data Security:
Consent decrees and settlements

Common themes in settlements relating to data security program requirements:

- Identify material internal and external risks to the security of personal information, including but not limited to assessments of:
  - employee training and management;
  - information systems, including network and software design, and information processing, storage, transmission, and disposal; and
  - prevention, detection, and response to attacks, intrusions, or system failures.
- Design and implement reasonable safeguards to control the risks identified through the risk assessment.
- Regularly test or monitor the safeguards' effectiveness.
- Designate an employee or employees to coordinate the information security program.
- Develop reasonable steps to select and oversee service providers that handle personal information.
- Evaluate and adjust the program to reflect the results of monitoring, material changes to the company's operations, or other circumstances that may affect program efficacy.
- Accountability and oversight by FTC:
- Designating senior manager to oversee program
- Prescriptive measures to safeguard personal information, including employee training, technical threat monitoring, access controls, and encryption
- Obtain third party assessments of programs every two years

Data Security:

FTC cases (sources)

- Chegg - In the Matter of CHEGG, INC., a corporation, January 26, 2023, FTC Matter Number 2023151
- Drizly - In the Matter of Drizly, LLC, January 10, 2023, FTC Matter Number 2023185
- CafePress - In the Matter of RESIDUAL PUMPKIN ENTITY, LLC, June 24, 2022, FTC Matter Number 1923209
- BetterHelp - In the Matter of BETTERHELP, INC., March 2, 2023, FTC Matter Number 2023169
- Available at: Privacy and Security Enforcement | Federal Trade Commission (ftc.gov)

Thank you!

Questions?

Elaine F. Harwell, CIPP/US, CIPM
Partner, Procopio
elaine.harwell@procopio.com
619.906.5780

Nick Ginger
Senior Vice President and Senior Counsel, City National Bank
Nick.Ginger@cnb.com
619.889.6851

Procopio