Cybersecurity Law Report
An Acuris company

cslawreport.com

March 31, 2021

OPERATIONS

How Do You Put a System of Controls in Place When Your Target Keeps Moving?

By Michelle Reed and Madison Gafford, *Akin Gump*

The nearly monthly changes to privacy and cybersecurity regulation at the federal, state and local levels have left businesses reeling on how to comply. On January 1, 2020, the first comprehensive privacy regulation – the California Consumer Privacy Act (CCPA) – became effective in the United States. Following that implementation, more than 75 class action lawsuits were filed related to CCPA alone. Nearly 20 states have introduced some form of comprehensive privacy and/or cybersecurity regulation. States and even cities across the nation have joined the fray of regulating biometric information, with resulting litigation settlements in the hundreds of millions of dollars, and Congress continues to debate comprehensive privacy and cybersecurity regulation.

The patchwork of privacy and cybersecurity regulation leaves businesses in a perpetual state of flux. To adapt to this ever-changing regulatory environment, businesses should develop a flexible framework with a system of controls based on core privacy and cybersecurity principles. Implementing this flexible framework allows businesses to get ahead of any future requirements so that a complete overhaul of corporate systems is not required.

See also "How Uber, eBay and Pitney Bowes Built Principles-Based Global Privacy Programs" (Oct. 16, 2019).

A Dynamic Legal Landscape

The dynamic nature of privacy law provides the backdrop to the need for flexible privacy and cybersecurity compliance programs. The United States has a long history of privacy protection. Before modern-day technology, the country's founders focused on unlawful intrusions into our homes and personal papers, forever enshrined in the Fourth Amendment. In more recent history, federal and state governments have issued many laws to address privacy issues.

Federal and Sectoral

Leading the way, the Federal Trade Commission Act (FTCA) provided broad consumer protection focusing on unfair and deceptive trade practices (15 U.S.C. §§ 41–58). The Act's purpose was to prevent companies from taking advantage of consumers by not posting privacy policies, sharing personal information, and failing to enforce any reasonable security measures.

Federal legislators also regulate high-risk industries on a sectoral basis. One well known example comes from the healthcare sector – the Health Insurance Portability and Accountability Act, 45 C.F.R. §§ 160, 164 (HIPAA) – that provided a series of laws and regulations related to patient privacy and data security. Congress continued its path of sectoral legislation with the passage of the Gramm Leach Bliley Act, 15 U.S.C. §§ 6801 et seq., which imposes privacy and security requirements on financial institutions that offer consumers financial products or services like loans, financial or investment advice, or insurance. The energy, marketing and advertising, and insurance industries are examples of other industries with self-created regulatory frameworks, such as the Interactive Advertising Bureau Standards and Guidelines, National Association of Insurance Commissioners and the Cybersecurity Capability Maturity Model (C2M2) Program.

National standards have also been developed and now are often used as benchmarks of reasonable privacy and security programs. The National Institute of Standards and Technology (NIST) issued its "Framework for Improving Critical Infrastructure Cybersecurity" in 2014 and updated it again in 2018. Its general purpose was to create a flexible framework, for businesses of all sizes, to improve cybersecurity risk management. This framework continues to be a model for what constitutes a "reasonable" security system. The "NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management" followed just a few years later in 2020.

See "NIST Privacy Framework: Insights on New Tool for Managing Privacy Risks" (May 6, 2020).

State Laws

The shift in state privacy regulation came in 2018, with the passage of the California Consumer Privacy Act, Cal. Civ. Code § 1798.150 (CCPA), which is a comprehensive privacy law that transcends former sectoral bounds. The CCPA created a private right of action for consumers residing in California to sue businesses that suffered data breaches involving the compromise of actionable private information. The CCPA importantly imposed affirmative obligations on companies to allow consumers the right to access information collected, to request that a business delete consumer information, of disclosure of the information collected, of disclosure of information sold, and to opt out of the sale of personal information. It disallows discrimination for exercising any of these privacy rights.

The shift in state cybersecurity regulation came in 2017, with the New York Department of Financial Services (NYDFS) implementing a comprehensive Cybersecurity Regulation that imposed minimum levels of security, with governance, training and third-party vendor management provisions, among many others. Shortly thereafter, New York passed the Stop Hacks and Improve Electronic Data Security (SHIELD) Act in 2019, imposing an array of data security and governance requirements on all companies conducting business in New York (not just those regulated by the NYDFS).

A cascade of privacy and cybersecurity regulation followed nationwide. In November 2020, California voters voted for a major overhaul of the CCPA, in favor of the California Privacy Rights Act of 2020 (CPRA), which will become operative January 1, 2023.

Then in March 2021, Virginia passed the Consumer Data Protection Act (VCDPA), which also becomes effective January 1, 2023. New York is now poised to pass state privacy regulation and Washington continues to debate a GDPR-like data privacy bill that is expected to eventually pass. More than 15 additional states have introduced legislation related to data privacy, including Alabama, Florida, Illinois, Iowa, Kentucky, Minnesota, Mississippi, Nebraska, New Mexico, New York, North Dakota, Oklahoma, Pennsylvania, South Carolina, Utah, Washington state and Wisconsin.

With the tidal wave of privacy and security regulation, it is imperative that businesses take action now to create a system of controls that is not only compliant, but is also effective against privacy and cybersecurity threats.

Putting a System of Controls in Place

Businesses should implement a system of controls to decrease risk of liability posed by data privacy incidents and cybersecurity breaches. Due to the changing nature of the law, setting up a system that complies with controlling data privacy laws may seem overwhelming.

With any framework, three general stages will help to cultivate these compliance mechanisms. First, businesses should look at what data it collects, processes and shares, paying particular attention to where it is transferred and how long it is stored. Second, based on its inventory, the business should start to make individualized decisions about how it wants to protect data. And third, the business should implement its plan throughout its entire enterprise, including educating employees on the new system and providing checks and balances to ensure compliance.

Information-Gathering Stage

The first step businesses must take is to create their data inventory. A business must have a clear idea of the type of personal information it collects and stores. This should include any private information from consumers, employees, and data bought or gathered from third-party vendors. The inventory should include the following:

- what personal information the business collects from employees, customers, households and devices (including whether it is sensitive data);
- when and how personal information is collected;
- where the information is stored and for how long;
- for what purposes the information is collected and/or shared;
- with whom the information is shared (including whether it crosses any international borders); and
- nature of transfers (sale, disclosure for business purposes).

Relatedly, a business should identify its weaknesses and operational challenges. It should survey its current compliance mechanisms and look back on any operational failures, including past data breaches and other mistakes. While looking at its own internal mechanisms, it is a good idea to survey peer organizations as well. Not all businesses have the same budget, store the same personal information or are part of the same business sector. Therefore, it is invaluable to scope out the competition and learn from their mistakes and mimic their successes.

See "Maintaining Privacy While Staying Competitive in an Evolving Regulatory Landscape" (Jan. 6, 2021).

Planning Stage

After a business finishes assessing its own internal structure, then it can begin to make decisions on how it wants to operate its compliance program.

Core Provisions

To create a flexible system of controls, it is important to make sure your privacy program addresses the following core provisions in most data privacy laws:

- individual rights (rights to access, correct, delete, portability, opt out/opt in);
- notice/disclosures;
- purpose limitation;
- data minimization;
- security requirements;
- privacy-by-design;
- risk/impact assessments;
- service provider requirements;
- automated decision-making and profiling;
- provisions for special types of data (children's data, health data, government contract data, and other sensitive data);
- governance (including privacy officer).

Highest Standard?

The business must also decide whether the privacy program will be unified to the highest standard or vary by country/state. It is important to remember that your determination of how to approach privacy will stay with the data for the life of the data.

For example, with advent of the GDPR and Canadian Anti-Spam Legislation (CASL), many businesses found that they had to completely rebuild marketing and other lists where they did not have proper consents and evidence of such consent. Opt-in consent, while potentially decreasing sign-ups in the short term, will provide longevity and stability to your data set in the long term.

Conversely, imposing an opt-in requirement in a jurisdiction not requiring opt-in consent may put the business at a competitive disadvantage. These risks must be considered and weighed by all stakeholders.

Third-Party Vendors

Third-party vendors often pose some of the most significant risk to any privacy or security program. Businesses must include statutorily required contractual protections and conduct and document solid due diligence before entering sharing data with any third party. Basic questions should include:

- What type of data will be shared with, collected by or accessed by the vendor?
- What is the vendor permitted to do with the data?
- Where will the vendor store the data?
- How long will the data be kept, and what are the protocols around deletion?
- What security controls does the vendor have in place?
- Does the vendor have good privacy-by-design so that privacy is favored by default?
- Does the vendor have incident response and disaster recovery plans?

Once the diligence is collected, it should be stored and refreshed on a regular basis.

See the CSLR's two-part series on privacy and security provisions in vendor agreements:

"Assessing the Risks" (Mar. 17, 2021); and "Key Data Processing Considerations" (Mar. 24, 2021.)

Critical Stakeholders

Making friends in the right places is crucial to a privacy or security program's success. Identifying compliance implementation leads and key stakeholders – those whose jobs will be impacted by the decisions you are making – is key to long-term success. Critical stakeholders should include team members from the digital, information technology, sales and customer service groups.

When planning, a company must also be aware of its capacity and appetite for change in determining what system and process will be used for the access, opt-out, consent, and deletion requirements. If it imposes a system that is too onerous, it is likely to be circumvented if the company has not achieved buy-in from each of the business units.

Implementation Stage

Implementation and data governance often poses the greatest challenge for businesses. To prevent data breaches and comply with controlling privacy and security law, the system of controls must permeate the entire business. Only focusing on the perceived highest risk areas (*e.g.*, technology departments or high-dollar-value contracts), leaves other areas vulnerable to security intrusions or mistakes. Sometimes it is the smallest vendor who poses the most significant privacy or security liability to a company.

"Gut Check" Approach

With strong leadership, implementing the compliance program can be the best way for businesses to reduce privacy and security risks. The chief privacy or information security officer should take implementation in stages, evaluating the highest risk areas for the business and then focusing on one area at a time. The "gut check" approach to privacy law can be useful—if something feels overly intrusive or creepy, there is probably a regulation that prevents that usage of data. Leaders must use common sense in evaluating and evolving privacy and security compliance programs.

Strong Teams and Regular Meetings

Recognizing the dynamic nature of privacy is key. A business's data inventory is typically out of date just weeks after it is completed, as new vendors are onboarded and business processes are changed. A new law could completely overhaul consent or rights requirements. Establishing solid privacy and security teams with a regular meeting schedule that addresses these changes and risks is essential. If strong privacy and security compliance tools are in place, the established governance committee can quickly and efficiently review any changes to the way data is used or to the laws that are applicable to the business and address any necessary changes.

Training

Employee training is also key to successful implementation of any privacy or security compliance program. Training should not be limited to initial onboarding. Employees should be trained at least annually, and ideally at varying points throughout the year through reminders and engaging video training. With large portions of the workforce working from home, training and holding individuals accountable is essential.

Specialized training to key departments – customer service, human resources, financial services, information technology, managers, marketing, sales, healthcare – will greatly reduce privacy and security risk. Reminding employees of the risks of noncompliance and detailing the damage that could occur if compromised is critical to establishing the importance of the compliance program. Other training methods can include random phishing drills or short virtual modules to help remind employees of the ever-present danger of cyber fraud scams.

See CSLR's three-part guide to cybersecurity training: "Program Hallmarks and Whom to Train" (Oct. 16, 2019); "What to Cover and Implementation Strategies" (Oct. 23, 2019); and "Assessing Effectiveness and Avoiding Pitfalls" (Oct. 30, 2019).

Periodic Testing

Policies and procedures must be tested. Internal audit or third-party risk assessors are essential to making sure that privacy and cybersecurity programs continue to mature with evolving risks.

Businesses should make sure that their programs and implementation are tailored to their actual practice. For example, many new privacy laws emphasize consumer consent and opt-out management systems. Simply posting a privacy-related disclosure on the business's website is insufficient. In addition to this disclosure, there needs to be a practical way for a consumer to "opt out" of having her private information stored on the business's server or shared with third-party vendors. Businesses have faced FTC and state attorney general scrutiny for instances where an "opt out" option is mentioned in a policy statement, but where there are no instructions or an actual way to take this course of action. Periodic testing will ensure that policies and procedures are followed and are not out of date with actual company practice, helping to decrease privacy and cybersecurity risk.

See "How eBay and PayPal Use Key Performance Indicators to Evaluate and Improve Privacy Programs" (Jan. 8, 2020).

Part of the Culture

Data privacy and cybersecurity law is a new frontier, with an ever-changing patchwork of regulation. Even though the target keeps moving, the principles underlying these laws and regulations remain the same: know what data you collect/process/share, disclose how you use it, and be mindful of protecting and minimizing the data you keep. With strong governance and regular testing, data privacy and cybersecurity compliance will become part of a business's culture.

See "How to Build a Cybersecurity Culture Using People, Processes and Technology" (Aug. 15, 2018).

Michelle Reed is co-head of Akin Gump's cybersecurity, privacy, and data protection practice and is based in Dallas. Reed advises companies, boards, and executives on navigating ever-changing privacy and cybersecurity regulation, enforcement, and class action litigation. She works across business units to find practical, compliant solutions for clients.

Madison Gafford is a litigation associate in the Dallas office of Akin Gump.