Laws governing cybersecurity and privacy have been in effect for a number of years in both Canada and the United States. Enforcement activities have been on the rise in both countries. Although the Canadian framework has one federal statute, supplemented by provincial laws, in the U.S. there are multiple federal laws and a growing number of state statutes and regulations that govern privacy and cybersecurity. Understanding the laws and regulations that are applicable to a business or client is imperative in order to assure that personal information and sensitive or confidential information are appropriately protected. For businesses that are engaged in Canadian-U.S. cross-border transactions it is important to have knowledge of laws and regulations on both sides of the border in order to assure that the personal and confidential information of individuals is protected while also minimizing risks to businesses that may occur through penalties for non-compliance with laws and as a result of possible loss of strategic business information through hacking activities or other loss of data.

In the U.S., no single federal law regulates the privacy and security of personal information and confidential data. Instead, there is a complex combination of federal and state laws and regulations that overlap and sometimes contradict one another. Recently, data breach disclosure obligations have expanded significantly as data security breaches continue to dominate the news. In addition, governmental agencies and industry groups have developed guidelines and self-regulatory regimes that create what amount to privacy and security best practices. These new laws, coupled with the tremendous increase in data collection and processing, result in greater risk of privacy and security violations and create significant compliance challenges.

The U.S. Federal Trade Commission Act, The Health Information Portability and Accountability Act (HIPPA), The Electronic Communications Privacy Act, and the Children’s Online Privacy Protection Act are several, but not all U.S. federal laws that govern certain actions or set out procedures that must be followed in order to protect private information as defined in the respective laws. The California Consumer Privacy Act and the Massachusetts Data Security Regulation are two state statutes that are trying to provide greater protection than may be available under federal laws. Washington State’s legislature is considering enacting a law called the Washington Privacy Act. If enacted, that law and the California act are two frameworks that are more stringent than other U.S. frameworks. The Washington legislation is more closely modeled after the European Union’s General Data Protection Regulation, which is more restrictive on businesses than current U.S. laws.

In Canada, PIPEDA (the Personal Information Protection and Electronic Documents Act) is a federal law that details how businesses must handle personal information. It is applicable to non-resident organizations, as well as those domiciled in Canada. Among the obligations
imposed by PIPEDA are the designation of a compliance officer, notifications to individuals and the government in the event of a data breach, and standards of security safeguards. Alberta, British Columbia and Québec each have provincial laws similar to PIPEDA that are applicable to private businesses. Some provinces also have laws that govern how health and employment related personal information must be handled. Businesses must develop policies that reflect the principles underlying PIPEDA. Development of a compliance program to implement those policies will be a significant step to further assuring that a business complies with PIPEDA and other applicable laws.

The Canadian Anti-Spam Legislation (CASL) addresses then manner in which electronic communications to consumers are to be handled. Concepts of consent and identifying the party sending notices are covered in the CASL. CASL requires that communications must include an unsubscribe feature. As is the case with PIPEDA, CASL applies to messages sent from outside of Canada to Canadian recipients.

Businesses should develop processes to assure compliance with applicable laws, regulations and standards regarding the collection, storage and dissemination of personal or confidential data. This paper summarizes some of the key privacy and data security laws in the United States, of which companies doing business in the United States from abroad should be aware, and which should inform a their compliance and risk management programs. It then provides practical recommendations of first steps to develop a culture of compliance.

Development of an effective compliance program requires commitment of mindshare and resources by the business leaders. All businesses should designate a person or team to be responsible for managing compliance programs. In a large business, a separate organization focused on compliance may be appropriate. The compliance person, team, or organization should have significant authority and status, with direct access to or be part of senior management, and should have direct access to the board. Leadership must embrace the concept that cybersecurity is an enterprise risk – not just the responsibility of the IT or security departments.

There should be an understanding that failure to develop and implement an appropriate program for compliance with privacy and cybersecurity requirements subjects the business to significant risks. Not only are there legal risks of for failing to comply with laws, including possible fines and third-party lawsuits, but there are risks to a business’ reputation, potential financial losses, harm to its network, and potential loss of a business’ intellectual property and/or strategic information.
Critical Cybersecurity Compliance Issues
for Canadian and US companies operating cross-border

Andrew Alleyne
2019 ABA Business Section Spring Meeting
[Date]
Statutory Schemes in Canada

**PIPEDA** – a federal privacy law that outlines how businesses must handle personal information

**Provincial Privacy Laws** – Alberta, British Columbia, and Quebec each have privacy laws, applicable to private corporations, that are substantially similar to PIPEDA

**Health/Employment Privacy Laws** – certain provinces also have health-related and employment-related privacy laws

**CASL** – Canada’s anti-spam legislation, which addresses electronic transmissions of information to consumers
Overview

PIPEDA – Key Features

Application – PIPEDA generally applies to the personal information of Canadian citizens held by private-sector organizations (including non-resident organizations)

Effects – If an entity holds personal information to which PIPEDA applies, the entity will have obligations relating to:

- the designation of a compliance officer
- notifications, to individuals and the government, in the event of a security breach
- standards of security safeguards
10 Principles – in order to comply with PIPEDA, an organization should attempt to follow these 10 principles (see Schedule 1 of PIPEDA):

1. Accountability
2. Identifying purposes
3. Valid, informed consent
4. Limiting Collection
5. Limiting use, disclosure, retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual access
10. Challenging compliance
Substantially Similar Legislation – if legislation, substantially similar to PIPEDA, already applies to personal information collected by an organization, the organization may be exempt from PIPEDA (i.e. certain provincial privacy statutes)

Non-profit Organizations – PIPEDA does not apply to organizations that are not engaged in commercial, for-profit activities

Public Information – PIPEDA does not apply to: information that is about an organization; information that has been rendered anonymous; or certain business contact information (among other exceptions)
Provincial Privacy Laws – Key Features

**Application** – in general, provincial statutes also apply to personal information held by private-sector organizations (although, definitions of “personal information” vary slightly).

**Effects** – If an entity holds personal information to which a provincial statute applies, the entity will have obligations related to:

- the consent of an individual (providing personal information)
- the use of obtained personal information
- the accuracy, protection, and retention of personal information
Health-related Privacy Laws – Key Features

**Application** – “health-related” privacy laws generally apply to the “personal health information” of Canadians collected by health care practitioners and service providers.

**Effects** – similar to the other privacy statutes, many provincial, health-related privacy statutes contain rules relating to:

- the receipt of consent from an individual
- the handling of records
- the appointment of a “contact person” responsible for statutory compliance
CASL – Key Features

**Substantially Similar Legislation** – CASL generally applies to persons sending commercial electronic messages to electronic addresses (e.g. emails)

**Consent and Identification** – CASL requires a business/organization to: (1) obtain the consent of a message’s recipient; and (2) clearly identify itself to the message’s recipient

**Unsubscribe** – Furthermore, CASL requires the inclusion of an unsubscribe mechanism in each sent electronic message

**Non-residents** – CASL applies to messages sent to recipients in Canada by a person or organization in a different country
**General Steps** – to ensure your organization is compliant with Canada’s privacy law legislation, one should take the following steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Determine what information you collect and how you collect/use it</td>
</tr>
<tr>
<td>2.</td>
<td>Ensure suppliers limit their use of information (e.g. via contract)</td>
</tr>
<tr>
<td>3.</td>
<td>Ensure you know with whom you share information</td>
</tr>
<tr>
<td>4.</td>
<td>Ensure systems are in place to record consent and its withdrawal</td>
</tr>
<tr>
<td>5.</td>
<td>Ensure security systems meet industry standards</td>
</tr>
<tr>
<td>6.</td>
<td>Ensure an appropriate process is in place for addressing breaches</td>
</tr>
</tbody>
</table>
10 Tips – The Office of the Privacy Commissioner of Canada has listed the following 10 tips for avoiding privacy complaints:

1. Post privacy officer’s contact info.
2. Train staff about privacy.
3. Take responsibility for employee actions.
4. Limit collection of personal info.
5. Make SINs optional.
6. Don’t record driver licenses.
7. Tell customers about video surveillance.
8. Protect personal information.
9. Respond to access requests.
10. Be up front about your collection and use of personal information.

Source: Office of the Privacy Commissioner of Canada, priv.gc.ca
Overview

PIPEDA – Key Features

**Requirement** – Organizations must develop policies that reflect the principles underlying Canada’s privacy legislation

**Topics to Address** – In order to comply with Canada’s privacy laws, an organization should develop policies that address:

- the collection, use, and disclosure of personal information
- access to and correction of personal information
- retention and disposal of personal information
- the responsible use of information and information technology

Source: Office of the Privacy Commissioner of Canada, priv.gc.ca
FASKEN
Best Practices for Cybersecurity & Privacy Compliance Programs

David Aschkinasi
March 29, 2019
Getting Started

• Development of an effective compliance program requires commitment of mindshare and resources by the business leaders
• All businesses should designate a person or team to be responsible for managing compliance programs
  • In a large business, a separate organization focused on compliance may be appropriate
  • The compliance person, team, or organization should have significant authority and status, with direct access to or be part of senior management, and have direct access to the board
Determine relevant laws and regulations that affect your business

- U.S.: Federal and State Laws and Regulations
  - Including but not limited to Federal Trade Commission Act, Health Insurance Portability and Accountability Act (HIPAA), Electronic Communications Privacy Act (ECPA), Children’s Online Privacy Protection Act (COPPA), California Consumer Privacy Act, New York Department of Financial Services Cybersecurity Regulation

- Canada: PIPEDA and Provincial Laws
  - Including but not limited to Personal Information Protection and Electronic Documents Act (PIPEDA), Personal Information Protection Acts (separate laws in Alberta, British Columbia and Québec), General Data Protection Regulation (European Union’s GDPR)

- European Union – General Data Protection Regulation (GDPR), Cybersecurity Act (expected to be formally approved and effective by Summer, 2019.)
Review standards or frameworks that apply to your business sector or would be helpful to your compliance program planning

*There is no single standard or framework that can be universally applied in a “check the box” approach – each business must determine what it needs – but…*

**These standards and frameworks may be helpful for guidance:**

- ISO 27001
- National Institute for Standards and Technology (NIST) Cybersecurity Framework
- Payment Card Industry (PCI) Data Security Standard
- North American Electric Reliability Corporation (NERC)
- Control Objectives for Information and Related Technologies (COBIT)
- Health Information Trust Alliance (HITRUST) Cyber Framework
- Center for Internet Security (CIS) Controls
Leadership must embrace the concept that cybersecurity is an enterprise risk – not just the responsibility of the IT or security departments.

- Legal risks
- Strategic risks
- Operational risks
- Financial risks
- Reputational risks

“Tone at the Top” is critical to assure that a compliance program is viewed as a critical business function, and not as requiring only perfunctory annual reviews.

Cybersecurity and privacy law compliance and accountability should be part of a corporate wide governance framework – it is important that responsibilities of all stakeholders are clear.
What are first steps to assuring a reasonable cybersecurity compliance plan?

- Conduct risk assessment
  - Assess data assets that the business has, and determine how important they are
  - Determine what level of protection exists for those assets
  - Identify gaps that exist between current level of protection and what is needed for adequate protection in view of the value of the assets
  - Determine the level of risk that the business is willing to take
- Develop processes and implementation plans to assure that gaps are closed
- Establish a plan for on-going assessments to provide monitoring and possible warnings of new gaps or risks
- Develop and implement training programs to educate management and employees about risks, security processes and compliance expectations
- Adopt an audit program to assure that monitoring, training and compliance are occurring
Third-Party Contractors May Create A Risk

- Well-intended compliance programs may be defeated by failures to account for the risk presented by third-party contractors or vendors
  - Vendors that have access to your internal systems may inadvertently or maliciously create data breaches or operational problems
  - An audit of third-parties’ systems and cybersecurity compliance programs can provide some indication of whether access to your systems by those parties creates unacceptable risks – audits of third-parties should be part of a compliance plan
  - A plan should be in place to assess the level of risk that is created by allowing access to internal systems for each vendor
  - Check vendor agreements to make sure that they include provisions requiring appropriate protection of data, audit rights and cooperation if a cyber event occurs
10 Privacy Tips for Businesses
(From the Privacy Commissioner of Canada)

With privacy becoming ever-more important to consumers, good privacy practices are good for business. Follow these tips to protect your customers’ personal information and comply with the federal law.

1. Get your customers’ consent to collect their personal information and limit your collection and retention of it.
2. Ensure staff receive appropriate privacy protection training.
3. Limit and monitor access to personal information and take appropriate action when an employee accesses information without authorization.
4. Think twice before collecting sensitive personal information, such as driver’s licenses.
5. Inform customers if you are using video surveillance.
6. Have a privacy policy and be upfront about your collection and use of personal information.
7. Protect personal information on laptops, USB keys and portable hard drives through technological safeguards such as encryption and password protection.
8. Respond to requests for access to personal information in a timely manner.
9. Safeguard personal information against privacy breaches and report breaches that could result in significant harm to an individual.
10. Make sure your customers know who to speak to if they have questions about privacy.
Canada Views Accountability as Critical to Ensuring an Adequate Privacy Program
(From the Privacy Commissioner of Canada)

• “Accountability in relation to privacy is the acceptance of responsibility for personal information protection. An accountable organization must have in place appropriate policies and procedures that promote good practices which, taken as a whole, constitute a privacy management program. The outcome is a demonstrable capacity to comply, at a minimum, with applicable privacy laws. Done properly, it should promote trust and confidence on the part of consumers, and thereby enhance competitive and reputational advantages for organizations…

• There will be times when mistakes are made. However, with a solid privacy management program, organizations will be able to identify their weaknesses, strengthen their good practices, demonstrate due diligence, and potentially raise the protection of personal information that they hold to a higher level than the bare minimum needed to meet legislative requirements.”
The touchstone of the Commission’s approach to data security is reasonableness: a company’s data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities. Through its settlements, testimony, and public statements, the Commission has made clear that it does not require perfect security; reasonable and appropriate security is a continuous process of assessing and addressing risks; there is no one-size-fits-all data security program; and the mere fact that a breach occurred does not mean that a company has violated the law.” (Commission Statement Marking the FTC’s 50th Data Security Settlement – January 21, 2014)

This approach was generally upheld in FTC v. Wyndham (799 F.3rd (3d Cir. 2015), a case in which the Third Circuit of Appeals held that the FTC does have authority to regulate data security, and further found that the Federal Trade Commission Act, in conjunction with guidance provided by the FTC, provides sufficient notice of standards of care that are enforceable. The Court stated that the FTC is not required to provide notice with “ascertainable certainty” of the cybersecurity standards by which the FTC expects businesses to conform.
Final Thoughts

- A strong compliance program needs buy-in and active support from the board and senior management.
- Understanding new technologies and continually reviewing and updating processes will help keep data protection/privacy compliance programs effective.
- Communications and training programs are essential for creating a culture of compliance.
- Be aware of external events and understand how they can affect your business.
About the GDPR…. (we are providing some information regarding compliance but we are not providing detail here about all of the requirements of the GDPR)

- You must have at least a basic understanding of the General Data Protection Regulation of the European Union if your business or your clients have or may have even a small relationship with any customers or businesses in European Union member states
- Regulation (EU) 2016/679 (GDPR) became effective May 25, 2018, and penalties for non-compliance have already been levied for non-compliance
Does the GDPR Apply to Your Business?

- If your business is established in any EU member state, the GDPR will apply.
- If your business is outside of the EU but is a data controller or data processor processing the personal information of EU residents, if it offers goods or services in the EU, or if it monitors behaviors of data subjects in the EU, then the business is subject to the provisions of the GDPR.
- If any of your vendors or service providers collect or process the personal information of EU residents on behalf of your company, the GDPR will apply.
A Quick Checklist for GDPR Compliance

- Does your company have an overall compliance plan and policies that represent the business’ commitment to comply with the GDPR?
- Are your employees, managers, and directors, as well as your suppliers, aware of the GDPR requirements and how your business handles data protection?
- Have you determined what data processing activities your business engages in?
- Have you conducted an assessment to determine the data protection processes that your business currently has in place?
- Using that assessment of existing data protection processes, have you determined if those processes comply with the GDPR requirements?
- If existing processes are insufficient to meet the GDPR requirements, do you have an implementation plan to remedy the deficiencies?
- Are the provisions of your supplier and vendor contracts sufficient to assure that your suppliers and vendors will comply with the GDPR requirements?
- Have you reviewed your customer contracts to determine if the provisions adequately reflect GDPR requirements? – especially regarding customer consent to processing personal data and your commitments regarding how you protect personal data.
- Do your business processes include data transfers outside of the EU? If yes, do you have adequate safeguards in place to comply with GDPR protections?
- Does your business have a process or processes that include documenting compliance activities and that will allow authorized parties to audit your business’ activities to assure compliance with the GDPR?
GDPR: Accountability is a Key Principle

- GDPR Article 5(2) states: “The (data) controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).” Paragraph 1 states operational principles.

- The following is from the Irish Data Protection Commissioner’s Website regarding becoming accountable for compliance with the GDPR:
  
  - Make an inventory of all personal data you hold and examine it under the following headings:
    - Why are you holding it?
    - How did you obtain it?
    - Why was it originally gathered?
    - How long will you retain it?
    - How secure is it, both in terms of encryption and accessibility?
    - Do you ever share it with third parties and on what basis might you do so?
  
  - This is the first step towards compliance with the GDPR’s accountability principle, which requires organisations to demonstrate (and, in most cases, document) the ways in which they comply with data protection principles when transacting business. The inventory will also enable organisations to amend incorrect data or track third-party disclosures in the future, which is something that they may be required to do.
David Aschkinasi
Glade Voogt Lopez and Smith, PC
Denver, Colorado

daschkinasi@gvlslaw.com
303-257-0676
WHERE TO START? COMPLIANCE WITH CROSS-BORDER CYBERSECURITY AND PRIVACY REGULATIONS IN THE U.S.

By William R. Denny
Potter Anderson & Corroon LLP
Wilmington, DE

February 15, 2019

The political consulting firm Cambridge Analytica harvested and used personal data of 87 million Facebook users in a manner that neither Facebook nor its users contemplated. This was not a hack, but nevertheless resulted in a major public relations scandal for the companies involved, and reportedly caused many customers to abandon the platform. In 2017, Equifax suffered a huge hack in which attackers gained access to the financial and personal information of at least 150 million people. The breach was expected to cost Equifax $439 million by the end of 2018, only a small portion of which was covered by insurance. Many financial institutions, private businesses and public agencies have had their networks frozen by ransomware. Data breach disclosure obligations have expanded significantly as data security breaches continue to dominate the news. Companies large and small are facing greater risks due to cyber-attacks, which create legal, financial, operational and reputational risks.

In the U.S., no single federal law regulates the privacy and security of personal information and confidential data. Instead, there is a complex combination of federal and state laws and regulations that overlap and sometimes contradict one another. Recently, data breach disclosure obligations have expanded significantly as data security breaches continue to dominate the news. In addition, governmental agencies and industry groups have developed guidelines and self-regulatory regimes that create what amount to privacy and security best practices. These new laws, coupled with the tremendous increase in data collection and processing, result in greater risk of privacy and security violations and create significant compliance challenges.

Businesses should develop processes to assure compliance with applicable laws, regulations and standards regarding the collection, storage and dissemination of personal or confidential data. This paper summarizes some of the key privacy and data security laws in the United States, of which companies doing business in the United States from abroad should be aware, and which should inform a their compliance and risk management programs. It then provides practical recommendations of first steps to develop a culture of compliance.

1. **Federal Laws.**


   The FTC Act is a broad consumer protection law that does not expressly address privacy and security, but empowers the FTC, among other things, to prevent unfair or deceptive acts or practices involving the collection, use, processing, protection and disclosure of personal information. The FTC has emerged as the primary federal regulator in this area and every company that does business in the United States falls within its jurisdiction. It brings
enforcement actions against companies for failing to comply with their posted privacy policies, for making material changes to their privacy policies without adequate notice to consumers, and for failing to provide reasonable security for sensitive customer information. Its settlements and consent decrees provide significant guidance as to the type of behavior the FTC expects. It also publishes data security guidance, including its Start with Security: A Guide for Business and its Stick with Security blog posts, which can be found at https://www.ftc.gov/tips-advice/business-center.


The GLBA is a sector-specific law that establishes privacy and security requirements for financial institutions. It includes the Financial Privacy Rule, 15 U.S.C. §§ 6801–6809, which regulates the collection and disclosure of private financial information, and the Safeguards Rule, id., which stipulates that financial institutions must implement written information security programs to protect such information.


HIPAA is also sector-specific, applying to medical service providers. Title II of HIPAA contains the Privacy Rule and the Security Rule. The Privacy Rule regulates the use and disclosure of protected health information (“PHI”) held by “covered entities,” which include health care providers, employer-sponsored health plans, and other medical service providers, as well as their contractors who fit within the definition of “business associates.” The Security Rule deals specifically with electronic PHI, and lays out administrative, physical and technical safeguards required for compliance. Administrative safeguards include policies and procedures designed to show how the entity will comply with HIPAA. Physical safeguards relate to physical controls that protect against inappropriate access to protected data. Technical safeguards relate to controlling access to computer systems and enabling covered entities to protect communications containing PHI from being intercepted by an unauthorized person.


Title I of the ECPA protects wire, oral, and electronic communications while in transit, while Title II, also called the Stored Communications Act, 18 U.S.C. § 2701 et seq. ("SCA"), protects communications held in electronic storage. The SCA protects the privacy of the contents of files stored by service providers and of records held about the subscriber by service providers, such as subscriber name, billing records, or IP addresses.


COPPA applies to the online collection of personal information about children under 13 years of age. It details what a website operator must include in a privacy policy, when and how
to seek verifiable consent from a parent or guardian, and what responsibilities an operator has to protect children's privacy and safety online, including restrictions on the marketing of those under 13. The FTC has authority to regulate and enforce COPPA. As of June 2016, the FTC has approved seven safe harbor programs, designed to encourage increased industry self-regulation. The FTC has issued rules defining what it means to “collect” data from children, and introducing data retention and deletion requirements. Under these rules, companies are also responsible for ensuring that any third parties to whom a child’s information is disclosed have reasonable procedures in place to protect the information.

Among other things, companies who collect data subject to COPPA must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of the personal information collected from children under age 13, including by taking reasonable steps to disclose such personal information only to parties capable of maintaining its confidentiality and security. They must also retain personal information collected online from a child for only as long as is necessary to fulfill the purpose for which it was collected and delete the information using reasonable measures to protect against its unauthorized access or use.


FCRA was enacted to promote the accuracy, fairness, and privacy of consumer information held by consumer reporting agencies. It has the distinction to be one of the first data protection laws passed in the computer age. Its regulations apply not only to consumer reporting agencies but also to users of consumer reports and to companies that furnish consumer information to reporting agencies. Typically, these are creditors and collection agencies.

G. Computer Fraud and Abuse Act, enacted in 1986 as an amendment to existing computer fraud law (18 U.S.C. § 1030) (“CFAA”)

The CFAA imposes both civil and criminal liability for a wide variety of acts that compromise the security of computer systems. It imposes liability on anyone who intentionally accesses a computer, including a cell phone, without authorization or in excess of authority, and in doing so steals anything of value, knowingly transmits a program or code that intentionally causes damage, knowingly traffics illegally in passwords, or threatens to damage a computer with the intent to extort anything of value.


The TCPA regulates the collection and use of telephone numbers for commercial purposes, and applies to both telephone calls and text messages. For example, it sets out rules governing the times of day when telephone solicitations can be made, maintenance of a do not call registry, information that a solicitor must give to the customers, and the use of automated telephone equipment. The TCPA permits private rights of action and provides for the recovery either of actual or statutory damages.
2. **State Laws**

There are hundreds of state laws governing the collection, use, protection, disclosure and disposal of personal information. These include unfair or deceptive practices statutes, data security statutes, data breach disclosure statutes, laws to protect the privacy of consumer financial information or personal health information, laws to limit the collection, use and disclosure of social security numbers and payment card information, negligence or privacy torts, safe destruction of documents containing personal identification laws, student data privacy laws, and employee data privacy laws.

Because of the inconsistent scope and obligations of laws at the state level, as well as the possible preemptive effect of federal laws, it is difficult for companies to chart a path toward full compliance with state privacy and security laws. Therefore, companies often look to the requirements of two states, Massachusetts and California, which are considered to have adopted some of the most rigorous privacy and security laws.

A. **California Consumer Privacy Act of 2018**

For years, individuals have become increasingly uncomfortable with the myriad ways that companies harvest and monetize their personal data, and have called on companies and legislators to do a better job at protecting their data privacy. Then, in March 2018, the Cambridge Analytica scandal broke. The public learned that private data was harvested from millions of Facebook users without their knowledge or consent. At the same time, companies involved in international transactions were coming to grips with the European Union’s General Data Protection Regulations (GDPR), which came into force on May 25, 2018. The GDPR further established data protection as a fundamental right in Europe and gave significant control over data back to the data subjects.

California has long taken the lead in the development of privacy law in the U.S., and in 2018 pressure built for greater protection for individuals’ privacy, in answer to Cambridge Analytica, the GDPR, and numerous high-profile data breaches. In May 2018, a California ballot initiative on data privacy collected more than 600,000 signatures in support of presenting the initiative to voters, nearly twice the number of signatures required to do so. Californians for Consumer Privacy led the campaign in support of the measure. Alastair Mactaggart, a San Francisco-based real estate developer, chaired the campaign. As of June 28, 2018, Californians for Consumer Privacy had raised $3.05 million, with 98.4 percent of funds from Mactaggart. Mactaggart’s interest in privacy began when he asked a Google engineer at a cocktail party if he should be concerned about the issue. Mactaggart recalled the engineer saying that if people knew what we knew about them, they’d be freaked out. That got him thinking that if the law required transparency, there would be change.

But ballot initiatives are an imperfect way to make public policy on a complex subject like data privacy. Before enactment, it can be difficult for stakeholders to help improve an initiative’s content. And after enactment, an initiative can be difficult to amend. Therefore, California legislators hoped to do better, but they faced a deadline. June 28 was the last day the initiative’s sponsor could remove it from the ballot, and the sponsor told the legislature that he would do so only if they passed data privacy legislation first. Legislators rushed to meet this
deadline, but that rush meant privacy advocates didn’t have much chance to weigh in before it was passed. The California Consumer Privacy Act of 2018 (CCPA) was signed into law on June 28, 2018, only a few days after it was first introduced to the California legislature.

The CCPA represents a seismic shift in how businesses in the U.S. will deal with personal information. It represents a continuation of California’s pioneering work in data privacy litigation, as well as a dramatic leap from the traditional approach toward privacy in the U.S., that of notice, to an approach strongly influenced by the GDPR to afford significant rights and controls to individual consumers. The CCPA, with its broad jurisdictional sweep, will require many businesses to re-design their data security and privacy practices to avoid potentially significant liability. Even companies beyond the reach of the CCPA would be wise to consider the guidance that it offers with respect to the collection and protection of personal data in specific situations that have not, until now, been regulated in the U.S.

i. What Is the CCPA?

The CCPA grants consumers the right to know what information companies are collecting about them, why they are collecting that data and with whom they are sharing it. It gives consumers the right to tell companies to delete their information as well as not to share their data. Businesses have extensive reporting and record-keeping obligations under the CCPA and consumers and the California Attorney General have broad remedies, including a private right of action in the event of a data breach that provides for statutory damages of up to $750 per individual per incident.

ii. When Does the CCPA Become Effective?

The CCPA becomes effective on January 1, 2020. Private rights of action are possible immediately, while enforcement by the California Attorney General cannot begin until the earlier of July 1, 2020, or six months after the issuance of implementing regulations. Despite the effective date being several months in the future, companies need systems in place now to track what data they collect, where and how it is stored and to whom it is shared, because, as of January 1, 2020, consumers will the right to demand information from companies holding their data going back 12 months. Companies that cannot produce the required information going back to January 1, 2019, may find themselves in violation.

iii. Who Must Comply With the CCPA?

The CCPA applies to “businesses” and “service providers.” A “business” is any for-profit legal entity that collects or sells personal information from or about consumers, conducts business in the State of California, and satisfies one or more of the following thresholds: (1) earns annual revenues in excess of $25 Million, (2) annually buys, sells, receives or shares for commercial purposes personal information of 50K or more consumers, households or devices; or (3) derives 50% or more of its annual income from selling consumers’ personal information. A “service provider” is any legal entity that “processes information on behalf of a business and to which the business discloses a consumer’s personal information for a business purpose pursuant to a written contract.” “Consumer” is defined broadly as any California resident, including employees, students, tenants, customers and even California residents temporarily living outside
of California. “Sells” includes any transfer of information, including to affiliates, for any valuable consideration, which may not be monetary.

iv. What Information Falls Under the CCPA?

a. Personal Information

The CCPA provides to the “personal information” of a “consumer.” Personal information is defined as information that “identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.” This includes the basics such as name, contact information, IP address, biometric information, geolocation data, financial information, health information. It also includes commercial information, including consuming history or tendencies, internet and other electronic network activity information, audio, electronic, visual, thermal, olfactory or similar information, professional or employment-related information, and even inferences drawn from any personal information.

The list of what constitutes personal information under the CCPA is very long, and includes some novel categories, such as a consumer’s appearance or a marketing profile that the consumer did not even create, and it is likely to grow. How these categories relate to our conventional understanding of what is private is an interesting theoretical question and one likely to spur debate as the concept of privacy changes over the ensuing years. But practically speaking, we seem to heading to a presumption that virtually any data point collected about an individual consumer is private.

There are, however, some exclusions. Personal information does not include publicly available information from government records, health information covered by HIPAA, clinical trial information subject to the Common Rule, sale of personal information to or from a consumer reporting agency, financial information covered by GLBA and information subject to Driver’s Privacy Protection Act.

The CCPA, however, creates an enormous loophole that threatens financial service companies. It provides that the exemption of non-public personal information governed by GLBA “shall not apply to Section 1798.150.” This carve-out from the exemption means that Section 1798.150 will apply to financial institutions, including to its non-public personal information governed by GLBA. The impact of this cannot be overstated. Section 1798.150 sets forth a private right of action for consumers to seek statutory damages of not less than $100 and not greater than $750 “per consumer per incident or actual damages, whichever is greater” if the consumer's information “is subject to an unauthorized access, exfiltration, theft, or disclosure as a result of the business’s violation of the duty to implement and maintain reasonable security procedures and practices.” In other words, GLBA-regulated entities will still be subject to millions of dollars of potential damages through class-action lawsuits if they experience a data breach.
b. Consumer

The CCPA defines “consumer” extremely broadly and not in the way that the term “consumer” is commonly understood. It means “a natural person who is a California resident” as defined in the California regulations, including any person in the state of California for other than temporary or transitory purposes, or domiciled in the state of California but outside of the state for a temporary or transitory purpose. Thus, California residents temporarily living outside of California nevertheless are protected by the CCPA.

Notably, the definition of “consumer” is not limited to someone who purchases a good or service from a business. Therefore, it presumably includes every individual, including employees of a business or a business’s vendors. This raises significant additional challenges to businesses in determining how to comply with the statute, as many of the requirements seem not logically to apply to employees.

v. Basic Rights Granted Under the CCPA

The CCPA creates four basic rights for California consumers:

- A right to know what personal information a business has about them, and where (by category) that personal information came from or was sent.

- A right to delete personal information that a business collected from them or to require that personal information not be shared.

- A right to opt-out of sale of personal information about them.

- A right to receive equal service and pricing from a business, even if they exercise their privacy rights under the Act, but with significant exceptions.

vi. Record-keeping and Disclosure Requirements

The CCPA imposes significant record-keeping obligations on businesses. They must (1) track consumer information from collection through sale or deletion, and (2) create a system to promptly respond to requests. The 12-month requirement requires every bit of potentially private information to be retained for a full year and to track how it is used both internally and by third parties. There must be at least two systems for receiving consumer requests, requests must be answered within 45 days plus one 45-day extension, and all systems must be designed to keep personal information private.

Requests from consumers must be verified as coming from the actual consumer. However, what is sufficient for verification is unclear. Businesses face the jeopardy that inadequate verification may cause them to disclose personal information to the wrong party, in effect a data breach. Also, there is a tension between the business’s need to retain sufficient data to demonstrate that it adequately verified the consumer and a consumer’s request that all of his or her data be deleted.
Businesses also have enhanced disclosure requirements. Privacy notices must describe consumer rights and how to exercise them, list categories of personal information collected, sold and disclosed in the prior 12 months and updated every 12 months, link to a “Do Not Sell My Personal Information” page, identify categories of third parties who will receive the personal information, and identify financial incentives offered by the business. To the extent that the CCPA includes employees within the definition of “consumers,” these enhanced disclosure requirements and opt-out requirements fundamentally change how businesses commonly deal with their employees.

vii. California’s Confusing Anti-Discrimination Rule

The CCPA broadly gives consumers a right against having to pay a different price for goods or services because they don’t share their information. But the CCPA also carves out two enormous exceptions. First, retailers remain free to offer “financial incentives” for sharing information, an exception clearly intended to encompass the already widespread practice of offering discounts or coupons to consumers who subscribe to mailing lists. To offer financial incentives, retailers must provide notice to consumers (but the law references sections with no notice requirements), consumers must give the retailers prior opt-in consent, which the consumers may revoke at any time, and incentives must not be “unjust, unreasonable, coercive or usurious.”

Second, the CCPA allows retailers to offer lower prices to consumers who share their information if the discount is “reasonably related to the value provided to the consumer by the consumer’s data.” It is deeply unclear how to interpret this value provision, an invitation to litigation. Business therefore are likely to stick with the broad-based, financial incentives that are plainly acceptable and wait until regulations or judicial decisions clarify the precise meaning of the nondiscrimination provision.

viii. The Right to be Forgotten

Consumers have right to request that a business delete from its systems the consumer’s personal information or to request that the information not be shared with third parties. However, the language of the statute suggests that this right only applies to information that the business collected directly from the consumer, thus creating the operational challenge to track the source of each piece of data. The right to ask that information not be shared may prove more difficult for businesses than simply deleting it altogether, especially since the term “third party,” as defined in the statute, includes virtually anyone, even parent or affiliated companies.

Business must also “direct any service providers to delete the consumer’s personal information from their records.” However, the definition of “service provider” is limited to entities with whom the business has a “written contract” that contains certain express prohibitions. The definition thus creates a potential adverse incentive discouraging companies from including express prohibitions required by the CCPA in the written contracts with their third party providers.

There are limited exceptions to the right to delete personal information. For example, a business need not delete a consumer’s personal information if the business needs it to “exercise
free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law.” Also, a business may keep personal information “to enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer’s relationship with the business.”

Deletion is a particularly tricky aspect of data privacy, because it raises First Amendment concerns. If a statute can compel an internet service provider to delete all copies of a post made by a data subject, it could take away the ability of others to re-post the information and comment on it.

ix. Financial Institutions Under the CCPA

The CCPA has a limited exclusion relating to financial information covered by the Gramm Leach Bliley Act (GLBA), but with two enormous caveats: (1) the definition of “personal information” is so broad that it reaches far beyond information covered by the GLBA, and therefore it is likely to apply to some of the data collected by financial institutions, and (2) the exclusion relating to information covered by the GLBA does not apply to the private right of action and statutory damages available to individuals in the event of a data breach.

Because of the broad definition of “personal information” under the CCPA, financial institutions would remain subject to the provisions and requirements of the CCPA for all activities falling outside of the GLBA, which could include information they collect online. The GLBA regulates financial institutions' management of “nonpublic personal information,” which is defined in 15 U.S.C. § 6809 as personally identifiable financial information: 1) provided by a consumer to a financial institution; 2) resulting from any transaction with the consumer or any service performed for the consumer; or 3) otherwise obtained by the financial institution. In contrast, the CCPA defines “personal information” as any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. It is not limited to financial information. The CCPA definition of personal information includes, for example, internet protocol addresses, browsing history, search history, biometric information, geolocation data, consuming histories or tendencies, professional or employment-related information, and inferences drawn from a consumer’s interaction with a website. “Inferences drawn” can include a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes. For all information relating to a California resident that is not financial information under GLBA, financial institutions will be subject to all of the reporting, disclosure and record-keeping requirements of the CCPA, and must have in place processes to respond to consumer requests.

B. Other California Laws

The California Online Privacy Protection Act of 2003 (“CalOPPA”) sets a high standard of disclosures for consumer-facing privacy policies. It requires operators of commercial web sites, online services or mobile apps that collect personal information on California consumers to conspicuously post a privacy policy and comply with its policy. The privacy policy must, among other things, identify the categories of personally identifiable information collected about site visitors and the categories of third parties with whom the operator may share the information,
and provide information on the operator’s online tracking practices. Operators are also required to disclose how they respond to do-not-track signals and other mechanisms that enable consumers to indicate their preferences regarding the collection of personal information. An operator is in violation for failure to post a policy within 30 days of being notified of noncompliance, or if the operator either knowingly and willfully or negligently and materially fails to comply with the provisions of its policy.

While CalOPPA does not specifically require consent for the collection or use of personal information, other California statutes do require express consent when using personal information, such as California’s financial privacy law, prohibiting the sharing or selling of personally identifiable non-public financial information without consent, and California’s medical privacy law, prohibiting using personal medical information for direct marketing purposes without consent.

California’s Data Breach Disclosure Law, Cal. Civ. Code §§ 1798.29 and 1798.82, was the first data breach disclosure law in the nation, passed in 2002. California’s law has been followed by similar laws in 49 other states, the District of Columbia and numerous other territories. This law requires a business or a government agency that owns or licenses unencrypted computerized data that includes personal information, as defined, to notify any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The type of information that triggers the notice requirement is 1) an individual's name plus one or more of the following: Social Security number, driver's license or California Identification Card number, financial account numbers, medical information, health insurance, or information collected through an automated license plate recognition system; or 2) user ID and password or other specified credentials permitting access to online accounts. California specifies the contents of the notice, and requires that the Attorney General be notified if the breach notice must be sent to more than 500 California residents. The law now requires the person providing notice of a data breach to make available identity theft prevention and mitigation services at no cost to the affected individuals for at least twelve (12) months if the breach exposed or may have exposed an individual's social security number, driver's license number or California identification card number.

California’s “Shine the Light” Law, Cal. Civ. Code §§ 1798.83-1798.84, allows consumers to learn how their personal information is shared by companies for marketing purposes and encourages businesses to let their customers opt out of such information sharing. In response to a customer request, a business must provide either: 1) a list of the categories of personal information disclosed to other companies for their marketing purposes during the preceding calendar year, with the names and addresses of those companies, or 2) a privacy statement giving the customer a cost-free opportunity to opt out of such information sharing.

Like many states, California has an Information Security Statute, Cal. Civ. Code § 1798.81.5, that requires that businesses that own, license or maintain personal information about a California resident implement and maintain reasonable security procedures and practices, to protect that information from unauthorized disclosure. Although “reasonable” is not defined in the California law, the California Attorney General released a data breach report on February 16, 2016, stating that “[t]he failure to implement all the [Center for Internet Security’s Critical
Controls that apply to an organization’s environment constitutes a lack of reasonable security” under California’s information security statute.

C. Massachusetts Data Security Regulation, effective March 1, 2010.

The Massachusetts General Law Chapter 93H and its regulations, 201 CMR 17.00, require that persons who store or use personal information about a Massachusetts resident develop a regularly audited, written information security program (a “WISP”) to protect personal information. The regulation establishes minimum standards to be met in connection with the safeguarding of personal information, and applies to information contained in both paper and electronic records.

The Massachusetts regulation acknowledges that the administrative, technical and physical safeguards documented in the WISP should be appropriate to (a) the size, scope and type of business of the person obligated to safeguard the personal information, (b) the amount of resources available to such person, (c) the amount of stored data, and (d) the need for security and confidentiality of the information.

Notwithstanding this flexible approach, the regulations list the minimum requirements for every WISP. These include:

- Designating one or more employees to maintain the WISP.
- Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks.
- Developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises.
- Imposing disciplinary measures for violations of the WISP.
- Preventing terminated employees from accessing records containing personal information.
- Overseeing service providers, by:
  - Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures; and
  - Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information.
- Reasonable restrictions upon physical access to records containing personal information, and storage of such records and data in locked facilities.
• Regular monitoring to ensure that the WISP is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information.

• Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices.

• Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

In addition to the requirements listed above for the contents of the WISP, the Massachusetts regulation requires that the person maintaining the WISP also maintain a security system covering its computers that, at a minimum and to the extent technically feasible, include the following elements:

• Secure user authentication protocols including control of user IDs and other identifiers; a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices; control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect; restricting access to active users and active user accounts only; and blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system.

• Secure access control measures that restrict access to records and files containing personal information to those who need such information to perform their job duties; and assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls.

• Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.

• Reasonable monitoring of systems for unauthorized use of or access to personal information.

• Encryption of all personal information stored on laptops or other portable devices.

• For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.

• Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.
• Education and training of employees on the proper use of the computer security system and the importance of personal information security.

D. Following CCPA, Numerous States Are Introducing Privacy Legislation

i. State of Washington

The State of Washington recently introduced the Washington Privacy Act (WPA), which would regulate businesses that collect, use and share the personal data of Washington residents. This would create huge compliance headaches for companies doing business in the United States, because it is not modeled after the CCPA, but after the European Union’s General Data Protection Regulation. Thus, it creates multiple similar but inconsistent requirements. It borrows from the GDPR’s definition of personal data, which is “any information relating to an identified or identifiable natural person.” This is narrower than the CCPA definition, but in other respects the WPA is broader in scope.

For example, the WPA grants broader consumer rights, including the right to object to processing and to restrict processing under certain circumstances. It would require the company controlling the data to stop using personal data for direct marketing when a consumer objects, but would allow further processing for a purpose other than direct marketing if the business could show a “compelling legitimate ground” to do so. It requires expansive disclosures regarding the use of profiling and artificial intelligence, and prohibits its use as the sole factor in decision-making where the profiling has a significant adverse effect on the consumer.

Similar to the GDPR but going even farther, the WPA would require all controllers of personal data to conduct and document risk assessments for each processing activity before engaging in that processing or whenever the company changed the processing in a way that would materially impact consumers. The companies, further, would need to gain “consent” for any processing that, based on the assessment, would create risks to the customer that would outweigh the interest of the company, other stakeholders and the public.

ii. Other State Privacy Bills

Eight states other than Washington have introduced bills that are largely copycats of the CCPA, but with numerous variations. If some or all of these pass, they will create the type of confusion that is prompting Congress to pass preemptive federal legislation. Bills have been introduced in Hawaii (SB 418), Maryland (SB0613), Massachusetts (SD 341), Mississippi (HB 2153), New Mexico (SB 176), New York (S00224), North Dakota (HB 1485), and Rhode Island (S0234).

These bills widely adopt the language and in most cases the structure of the CCPA, thus exposing these laws to many of the same interpretation challenges that exist with the CCPA. The most significant divergences are in the area of enforcement. Three of the states (Mississippi, New Mexico and Rhode Island) would extend a private right of action to any unauthorized disclosure of personal information. Massachusetts would extend a private right of action to any violation of its privacy law. All of the laws require disclosure of specific rights available to
consumers, which could have the effect of requiring businesses to design different disclosures for different states.

E. New York Department of Financial Services Cybersecurity Requirements for Financial Services Companies, 23 NYCRR 500, effective March 1, 2017 (“NY DFS Cybersecurity Requirements”)

While the NY DFS Cybersecurity Requirements expressly apply to all financial institutions licensed by the New York Department of Financial Services and their third party service providers, the requirements have achieved a much wider reach by becoming a *de facto* standard. The Requirements impose strict cybersecurity rules on covered organizations, including the requirement to maintain a detailed cybersecurity program designed to protect the confidentiality, integrity and availability of the entity’s information systems, to implement and maintain a written cybersecurity policy, to designate a Chief Information Security Officer (CISO), to enact a comprehensive cybersecurity policy, to conduct a detailed risk assessment, to initiate and maintain an ongoing reporting system for cybersecurity events, and to establish a written incident response plan designed to promptly respond to and recover from any cybersecurity event. The Cybersecurity Requirements can be found here: [http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf](http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf).

3. **Movement toward a United States Privacy Law**

The vastly expanded rights afforded to California residents and the onerous obligations imposed on businesses by the CCPA, together with the influence of the GDPR on American companies engaged in international commerce, are propelling the U.S. Congress toward creating a federal privacy framework. Big tech companies are pushing for a federal bill to preempt California’s law. But California Attorney General Xavier Becerra warned on November 28, 2018, that Congress should not pass a relatively weak online privacy bill to protect consumer data and use it to take precedence over a new California law. U.S. lawmakers have introduced multiple privacy bills.

Various industry and consumer groups have ramped up their lobbying efforts to persuade Congress to adopt a new and pre-emptive privacy framework before more states follow the California model and possibly add even more onerous requirements. The pressures building to enact such legislation include the multiple, inconsistent state and sectorial federal laws governing privacy in the U.S., the broad reach of the GDPR and its effect on business practices, and the radically new approach to privacy taken by the CCPA.

There appears to be a growing consensus about the broad parameters of a new federal law. As with the GDPR and the CCPA, a new federal law would likely require transparency in how information is being collected, used, shared and stored. Consumers would require real notice and content to use and share personal information and have the flexibility to move data between services. However, it is unclear what the breadth of the definition of personal information would be, and what would be required for consent.

However, the challenges to adopting any federal legislation are numerous, and many interest groups, most notably the giant data companies Facebook, Amazon and Google, are
already heavily lobbying. Certain international businesses and perhaps the FTC would want the federal legislation to meet the GDPR adequacy standard, which would facilitate international data transfer. Other businesses would want an easier privacy standard, and would want that new standard to preempt the U.S. sectorial approach, including state laws such as the CCPA. The most significant issues currently appear to be (1) whether the new federal privacy law will preempt state law, and (2) whether there will be a private right of action.

A. Fight Over a Private Right of Action

A private right of action would allow consumers to sue data controllers and may include class action lawsuits on behalf of multiple consumers. Damages under such scenario could be huge. Privacy advocates would favor private rights of action, because federal and state regulators simply will not have the resources to police privacy laws effectively. On the other hand, most businesses would see class actions as unwarranted expenses that would benefit no one. Even meritless cases may be settled for large amounts if they survive the motion to dismiss stage, principally benefiting only the plaintiffs’ lawyers.

A likely outcome might be to allow state AGs to enforce the federal law in addition to the federal agency, probably the FTC, charged with enforcement. The FTC is likely to be given explicit rulemaking authority and additional resources to focus on enforcement. One possibility that would allow private rights of action would be for the law to include some significant barriers to private actions but to allow them under certain limited circumstances. There might be monetary damage limits as well.

B. Federal Preemption

The business community is looking to a new federal standard to preempt the CCPA and other state laws that impose multiple and inconsistent requirements on them. On the other hand, consumer groups feel that the new federal standard should represent a floor on compliance obligations and not a ceiling, and that therefore states should be free to impose additional protections for data privacy. Some states may attempt to get around preemption in the way that California is seeking to circumvent the FCC’s ruling ending net neutrality. They may restrict their own state governments from contracting with companies that are not complying with some stricter privacy standard. Thus, states with significant market influence could us the market to impose their own higher standards.

C. Disagreements within the Business Community

Larger, multinational companies would want the U.S. to move toward international data protection standards, which to them would be the least costly solution and would facilitate data flow across borders. On the other hand, smaller or more localized companies would prefer a weaker federal law that would impose fewer obligations and would totally preempt state law. Then the third faction, consumer groups, will want to get as much protection as they can get. Lobbyists for all groups will be active.
No matter what the contours of the eventual federal legislation, the EU will decide for itself whether the new U.S. law meets the adequacy standard of the GDPR. It is unlikely that the EU will give the U.S. the benefit of the doubt.

D. Proposed Framework from the NTIA

4. Notable Recent Privacy Proposals

A. National Telecommunications and Information Administration (NTIA) Proposal, September 2018

In September 2018, NTIA proposed and sought comment on a national approach to consumer privacy. It identified a number of privacy outcomes that should be produced by any federal privacy framework. These included: transparency of privacy policies; reasonable control by users of their data; reasonable minimization of the data collected and used by organizations; data security; user access to and ability to correct their data; management and mitigation of the risks of harmful uses or exposure of personal data; and accountability of organizations collecting and using data.

NTIA further issued a set of high-level goals that any national privacy framework should pursue. These include: harmonize the regulatory landscape, which currently involves a patchwork of competing and contradictory baseline laws; comprehensive application to all private sector organizations that collect, store, use or share personal data that are not covered by sectoral laws such as HIPAA; interoperability with international frameworks and norms; FTC as the federal agency to enforce consumer privacy; and scalability, i.e., different approaches for small businesses that collect little personal information, distinctions between controllers and processors.

By mid-November, more than 200 individuals, government entities and companies had submitted recommendations regarding what should and should not be done with respect to consumer privacy. Not surprisingly, the focus of many comments was on the GDPR and the CCPA. The European Commission (EC) submitted comments, predictably advocating for better integration and reconciliation of disparate privacy laws, which would provide more certainty to businesses and better transparency and predictability to consumers. The EC did recommend greater attention on two principles present in the GDPR that were absent from the NTIA proposal, namely (1) requiring consent or other lawful bases to process data, and (2) specifying a purpose for data processing.

There were numerous points of consensus, including support for the espoused outcomes as general guiding principles for any federal privacy law, support for goal of reducing fragmentation in U.S. privacy and data protection laws and bringing greater harmony to regulatory landscape; support for the law applying across all sectors of the economy, rather than being limited to a particular type of company; support for the FTC playing the leading enforcement role, and a risk-based approach indicates that enforcement and remedies should be proportional to potential harm.
However, there were numerous points of divergence. These included whether the new federal privacy law resemble GDPR and whether there should be preemption. Private companies and industry groups who wanted the law to be less restrictive than the CCPA mostly favored preemption. Other organizations worried that preemption would invalidate a host of existing protections for sensitive information like social security numbers, student data and more.


Senator Wye’s bill proposes to expand consumers’ privacy rights to review information companies have about them, to know which third parties are receiving their data, to challenge inaccuracies, and require companies to conduct impact assessments for their high-risk automated decision systems. It would amend the FTC Act to recognize non-economic injury, encompassing business practices that create a “significant risk of unjustified exposure of personal information.” It would establish a national Do Not Track system for consumers to opt out of their data being shared with third parties, provide for non-discrimination against opt-outs but allows companies to offer paid versions of their products and services as an alternative to giving up data, authorize the FTC to create regulations to establish and implement minimum data privacy and security standards and establish resolution mechanisms for consumers’ complaints, impose civil penalties of up to $50,000 per violation and 4% of an organization’s annual revenue, require annual reports to be filed by large companies on their privacy and security compliance measures, and provide for the possibility of 10-20-year jail sentences for some violations.

C. The Data Care Act, introduced by Sen. Brian Schatz (D. Hawaii) on December 12, 2018.

Senator Schatz’s bill would create fiduciary duties, requiring “online service providers” to “fulfill the duties of care, loyalty and confidentiality” to end users. The duty of care would require that businesses must “reasonably secure individual identifying data from unauthorized access and promptly inform users of data breaches.

The duty of loyalty would prohibit businesses from using individual identifying data in a way that would “benefit the online service provider to the detriment of an end user,” “result in reasonably foreseeable and material physical or financial harm to an end user,” or “be unexpected and highly offensive to a reasonable end user.” The duty of confidentiality would impose restrictions on the disclosure and sale of individual identifying information to third parties. A violation of the duties would be treated as a violation of the FTC Act and be subject to monetary penalties, and the FTC would be granted rulemaking authority to implement the act, and the law would not “modify, limit or supersede” other federal or state laws on privacy or security.

D. American Data Dissemination Act, introduced by Sen. Marco Rubio on January 16, 2019

Senator Rubio’s bill gives Congress, and not the FTC, the ability to write federal privacy rules that would override stringent state regulations. It mandates that the FTC recommend to Congress what privacy rules should apply, and prescribes hat they resemble those found in the
Privacy Act of 1974. The FTC must find a way to exempt smaller, newly formed entities from the rules, and must create a way for consumers to access records held by companies, and to correct a record if the user can show that it is not “accurate, relevant, timely or complete,” terms the FTC must define. The law would be enforced by the FTC, and it would preempt state law.

E. Innovative and Ethical Data Use Act of 2018, proposed by Intel Corporation.

This framework, proposed by Intel, would limit the use of personal information to purposes for which the consumer provides explicit consent, uses that are consistent with the original purpose, and as required by law or regulation. It would allow users to provide meaningful consent for data use and create mechanisms whereby they can make informed choices. Organizations must “narrowly and specifically” describe their purpose for data collection, while making room for individuals to object to errors or to the holding of data whose use may “disproportionately cause harm.”

The framework would require “robust” data security safeguards that are appropriate to the size and complexity of the covered entity, the nature and scope of the covered entity’s activities and the sensitivity of any personal data that is processed. It would also grant more enforcement authority and resources for the FTC, including “meaningful but fair” sanctions. Civil penalties up to $16,500 per individual for whom the covered entity unlawfully processed information, with aggregate limit of $1 billion per violation. There would be a safe harbor for companies that certify they are in compliance with the act, and it would preempt state privacy and data security laws.

F. The Data Broker Accountability and Transparency Act, HR 6548, introduced July 26, 2018, by Rep. Hank Johnson (D. Ga.), applies to “data brokers” and provide consumer rights that are similar to those under the GDPR and the CCPA.


This bill aims to introduce additional privacy-related rights and protections to social media and online platform users. It creates rules on transparency for providing terms and conditions of use and of the privacy and security program and the rules for changing them and provides users an opportunity to easily withdraw their consent, the right to access their information and to see a list of third parties that have received personal data.


Senator Warren’s bill would create an Office of Cybersecurity within the FTC, tasked with implementing and overseeing the law. It would addresses system and network security, network management and monitoring, application management and data security, and would apply not just to credit reporting agencies, but to any collected database of typical consumer data that is used for almost any purpose and communicated to another party. There would be a duty to inform Office of Cybersecurity about company’s cybersecurity measures, demonstrate that they follow reasonable data security practices and notify it of data breaches within 10 days of breach.

K. The Internet Bill of Rights Principles, Introduced by Rep. Ro Khanna (D. Cal.), incorporates GDPR-like provisions such as data portability, the right to access and the right to be forgotten, in addition to provisions regarding anti-discrimination, net neutrality and accountability.

5. Considerations for Developing a Data Privacy and Security Compliance Framework

Risk is much broader than legal compliance. Customers are concerned that their information has been stolen, manipulated, or used in unacceptable ways. Such reputational risk may result in the loss of brand value, which can be an existential threat to many businesses. Although Facebook did not suffer a data breach, the use of its data by Cambridge Analytica caused a substantial breach of trust. Theft of intellectual property also has grown tremendously but frequently goes unnoticed as companies lose the crown jewels of their organization. Supply chain risk can threaten business operations when an attacker infiltrates a business through one of its vendors. This risk applies not only to immediate vendors but second and third-tier vendors as well. The intent of an attack may not even relate to data theft but, instead, may be intended to impact business valuation or to drive down share prices. For example, Yahoo’s valuation fell by hundreds of millions of dollars when its breach was disclosed, effectively reshaping an impending sale of the company.

How should companies doing business in the United States address these risks? Cybersecurity is no longer just an IT issue—it is also an enterprise issue. Compliance programs should comport not only with legal requirements but also with current technology and market expectations. It is no longer sufficient to rely on physical and logical security controls alone.

A. Security Standards

In the past, information security compliance plans were often viewed through the prism of published standards. As the number of frameworks and standards has expanded, businesses can no longer rely on a “check the box” approach. Rather, each business should determine the types of risk it faces and develop a program to meets those specific needs.

The most commonly used standards include the NIST Framework for Improving Critical Infrastructure Cybersecurity, the Center for Internet Security (CIS) Critical Security Controls, and ISO/IEC 27001/27002.
The NIST Framework provides a framework of computer security guidance for how private sector organizations in the United States can assess and improve their ability to prevent, detect, and respond to cyber-attacks. The Framework organizes its “core” material into five functions, which are “Identify,” “Protect,” “Detect,” “Respond” and “Recover.” Each function is then broken down into numerous categories and subcategories. The goal of the Framework is to assist a company in understanding its current cybersecurity profile, defining its target profile, or where it would like to be in its cybersecurity, and creating steps to close the gap between its current and target profiles.


The CIS Critical Security Controls (https://www.cisecurity.org/controls/) are a recommended set of actions for cyber defense that provide specific and actionable ways to defend against attacks. The Controls attempt to prioritize a smaller number of actions that are designed to have the greatest results. The Controls derive from the most common attack patterns highlighted in the leading threat reports and vetted across a very broad community of government and industry practitioners.

ISO/IEC 27001, entitled “Information Technology-Security Techniques-Information Security Management Systems-Requirements,” is an information security standard, last published in September 2013 by the International Organization for Standardization and the International Electrotechnical Commission. This standard specifies a management system that is intended to bring information security under management control and gives specific requirements. Organizations who implement these requirements may be certified by an accredited certifying body as evidence of the quality of its controls.

The ISO/IEC 27001 standard is similar to other standards mentioned here, in that it requires the organization systematically to examine its information security risks, design and implement a coherent and comprehensive set of information security controls, and adopt a management process to ensure that the information security controls continue to meet the organization’s information security needs. ISO/IEC 27002, entitled “Code of Practice for Information Security Controls,” works in tandem with ISO/IEC 27001, and provides best practice recommendations on information security controls.

B. Roadmap to an Effective Privacy and Security Program

The most important component to any data privacy and security compliance framework is leadership. A culture of compliance is important and cannot be built by one person, one department or one technology. The tone from the top is crucial to ensuring that a compliance framework is effective. Policies and procedures do not mitigate risk unless people are held accountable for following them. Instead of trying to reconcile multiple frameworks, it is most useful to pick one, implement it, and—most importantly—actively manage it and audit the results.
Regardless of the framework selected, a roadmap to an effective data privacy program should include the following:

- **Assess the current state.** Assess what data you have, how it is used and where it is stored. Identify applicable laws and regulations. Understand the key risk drivers and business strategies, evaluate technical capabilities, existing policies, procedures and personnel.

- **Perform a gap analysis.** Identify and quantify gaps in controls, processes, resources and personnel. Then prioritize those gaps for remediation.

- **Develop an action plan to address needs.** Ensure that you have involvement from key business leaders and across functions. Define roles and responsibilities, as well as authority to make decisions. Develop plans for data security, third party risk management, training and incident response.

- **Update appropriate risk management policies, standards and processes to assure data security.** Policies should align with business strategies and should balance business objectives with the risks of collecting and managing personal information.

- **Establish and implement effective information risk management reporting.** The reporting should be timely, accurate, meaningful and actionable.

- **Monitor, adapt and revise the information security program to align to the rapidly changing threat landscape.** Periodically test incident response protocols, and audit compliance with policies and procedures. Ensure ongoing training, adapted to current risk profile and personnel.

For a business to implement a compliance program effectively, leadership must communicate that compliance is important. Encourage business leaders to understand that security is a key element to business continuity. Look at what data you collect, who can access it, what is the value to the business and whether adequate protections are in place. Also, even for the largest companies, sharing information with other businesses and with governmental and law enforcement agencies may be an important part of the risk mitigation strategy, allowing businesses to stay current with information about the most recent threats and bad actors.

i. **Establish Clear Roles, Responsibility and Accountability**

Because data privacy and security depends on collaboration among multiple stakeholders, make sure that each part of the compliance workflow has an assigned internal stakeholder and that each stakeholder knows his or her roles and responsibilities. For example, who is responsible for assuring that data protection is engineered into new product development? What is the plan for handling succession if you terminate your data security officer? How do you manage performance issues for personnel with access to sensitive information or who are responsible for implementing privacy controls? Who makes the decision to inform investors about material cybersecurity risks and incidents? Who makes the decision to take major
networks or processes offline during an incident? Make sure that you have the right people at the table. Otherwise, you may miss critical issues.

Every employee has a role to play in data security risk mitigation, so an effective compliance program must include ongoing training on policies, procedures and best practices. To be effective, training should be role-dependent and should be presented regularly but not so frequently as to cause employees to stop paying attention. Careless employees present a significant risk of business email compromise.

ii. Monitor, Communicate and Improve

Businesses should actively monitor technology, people and processes to assure compliance with policies and procedures and look for improvement opportunities. Communication should be consistent within an organization, both horizontally and vertically, and with third parties so personnel do not become complacent. To respond effectively to incidents, businesses should maintain active relationships with external experts and involve them in exercises. Create a learning culture of continual assessment of events and findings to avoid repeating the same mistakes. These steps will not eliminate risk or guarantee compliance, but they will establish a solid foundation for secure operations in an age of disruption.

C. FTC “Stick with Security”

The Federal Trade Commission has published significant guidance to companies relating to data security. Because the FTC is the foremost regulatory agency enforcing privacy and security laws, companies should take heed of its guidance. The most helpful general guidance regarding data security are “Start with Security: a Guide for Business,” released in 2015 (https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business), and “Stick with Security: A Business Blog Series,” released in 2017 (https://www.ftc.gov/tips-advice/business-center/guidance/stick-security-business-blog-series). Together, these documents offer insights into ten actionable principles and practical tips, taken from the FTC’s 60+ data security enforcement actions, that companies of any size and in any sector can take. These ten principles are:

- Start with Security, including not to collect personal information you don’t need, hold onto information only so long as you have a legitimate business need, and don’t use personal information when it’s not necessary.
- Control Access to Data Sensibly, including to restrict access to sensitive data and limit administrative access.
- Require secure passwords and authentication, including to insist on complex and unique passwords, store passwords securely, guard against brute force attacks and protect against authentication bypass.
- Store sensitive personal information securely and protect it during transmission, including to keep sensitive information secure throughout its lifecycle, use industry-tested and accepted methods, and ensure proper configuration.
• Segment your network and monitor who’s trying to get in and out.

• Secure remote access to your network, including to ensure endpoint security and put sensible access limits in place.

• Apply sound security practices when developing new products, including to train your engineers in secure coding, follow platform guidelines for security, verify that privacy and security features work, and test for common vulnerabilities.

• Make sure your service providers implement reasonable security measures, including to put vendor obligations in writing and verify compliance.

• Put procedures in place to keep your security current and address vulnerabilities that may arise.

• Secure paper, physical media, and devices.
David Aschkinasi
Special Counsel
Glade Voogt Lopez and Smith PC
Denver, Colorado

My practice focuses on corporate compliance issues and risk analysis, especially regarding cybersecurity, privacy, FCPA and international regulatory and trade matters. I provide support on domestic and international commercial transactions and federal government transactions.
William R. Denny  
Partner

Mr. Denny practices primarily in the areas of cybersecurity, data privacy and information governance. Bill is a Certified Information Privacy Professional (CIPP/US) through the International Association of Privacy Professionals (IAPP) and Chair of the IAPP KnowledgeNet Chapter for Delaware. He has represented public and privately held companies and government entities in a wide range of technology and intellectual property-related transactions, including counseling clients on compliance with cybersecurity laws, development of data security policies, contracting with cloud service providers, outsourcing of IT services, mergers and acquisitions, technology licensing, software development, sales of internet domain names, and website terms of use and privacy policies. Clients include major licensees of information technology as well as internet service providers, software developers and system integration service providers.

Bill has litigated disputes over the interpretation and enforcement of many types of technology contracts, general commercial contracts and liability insurance policies. He has tried jury and non-jury cases in federal and state trial and appellate courts, before arbitration panels, and by use of other alternative dispute resolution techniques.

Bill writes extensively on technology and business issues, including:

- “Standing and the Circuit Court Split in Data Breach Litigation” in Corporate Disputes, January-March 2018
- “Representations and Warranties in M&A Agreements” in the ABA’s Guide to Cybersecurity Due Diligence in M&A Transactions, December 2017
- “What’s Changed Under Delaware’s New Data Breach Law” in Law360, August 24, 2017
- “Building Your Cyber Incident Response Plan” in Delaware Business, May/June 2017
- “Cybersecurity as an Unfair Practice: FTC Enforcement under Section 5 of the FTC Act” in Business Law Today, June 2016

Bill frequently speaks at seminars, programs and meetings on topics including technology, e-discovery and cybersecurity, among others:
November 9, 2016: at a program sponsored by the Delaware State Bar Association, Mr. Denny presented “Recent Developments in Data Security.”

September 28, 2016, at a program sponsored by the Delaware Small Business Development Center, Mr. Denny presented “Data Breach and Vendor Risk Management.” This presentation focused on necessary due diligence, essential contract terms and follow-up activities to minimize the risk of harm caused by a vendor cybersecurity event.

September 7, 2016: 2016 Secure Delaware Workshop, Mr. Denny presented "Data Breach and Vendors: Strategies to Limit Your Risks of Data Breach and Protect Yourself from Vendor Vulnerabilities."

December 15 and 16, 2015: National Business Institute Seminar entitled “Legal Ethics of Email.” Mr. Denny was one of two principal speakers.


September 29, 2015: Delaware Cyber Security Workshop, “Changing Legal Landscape in Cybersecurity: Implications for Business.” Mr. Denny focused on recent developments in cybersecurity laws and regulations at a full-day seminar sponsored by the State of Delaware.

May 6, 2014: Delaware Cyber Security Workshop. “Changing Legal Landscape in Cybersecurity: Implications for Business.” This presentation focused on the latest developments and implications for businesses as they seek to protect their critical infrastructure and comply with laws and regulations for data protection.

April 10, 2014: ABA Business Section Spring Meeting, Cloud Computing and IT Services Subcommittee. Mr. Denny presented on recent developments in cloud computing contracting practices.

February 6, 2013: Delaware Cyber Security Workshop. Mr. Denny led a roundtable discussion on data security and data breach notification laws at the full day conference on cybersecurity sponsored by the State of Delaware.

January 2013: Technology Inn of Court of Wilmington. Mr. Denny led a panel discussion on e-discovery.

October and November 2013: Client presentations on indemnification and limitation liability provisions in commercial contracts.
PUBLICATIONS

Denny and Noa Contribute to Bloomberg Law Profile on Privacy and Data Security in Delaware
January 2018

Denny and Noa Highlight Standing Issue in Data Breach Litigation
December 20, 2017

Denny Contributes Chapter to ABA Guide to Cybersecurity Due Diligence in M&A Transactions
December 14, 2017

What's Changed Under Delaware's New Data Breach Law
Law360, August 24, 2017

Building Your Cyber Incident Response Plan
Delaware Business, May/June 2017

Cybersecurity as an Unfair Practice: FTC Enforcement under Section 5 of the FTC Act
Business Law Today, June 2016

RECENT NEWS

30 Potter Anderson Attorneys Named to the 2019 Best Lawyers® List
August 15, 2018

Denny Appointed to ABA Cybersecurity Legal Task Force
July 30, 2018

Denny Named IAPP KnowledgeNet Chapter Chair for Delaware
March 23, 2018

Denny Named Among Top E-Discovery/Technology Lawyers by Delaware Today
November 3, 2017

CLIENT ALERT: Update to Delaware Data Breach Disclosure Law
August 17, 2017

22 Potter Anderson Attorneys Named as "The Best Lawyers in America" for 2018
August 15, 2017

William Denny Earns CIPP/US Certification from the International Association of Privacy Professionals
June 6, 2017

Three Potter Anderson Attorneys Named “Lawyers of the Year” and 21 Attorneys Named as “the Best Lawyers in America” for 2017
August 15, 2016

Potter Anderson Attorney Comments on Delaware Federal Court Standards
February 2, 2012
RECENT EVENTS & SPEAKING ENGAGEMENTS

Denny to Speak on Cross-Border Cybersecurity Compliance Issues at ABA Business Law Section Meeting
March 29, 2019

Denny Presents at ABA Cyberspace Law Institute on Push for Federal Data Privacy Standard
January 25, 2019

Denny Presents on California Consumer Privacy Act
November 13, 2018

Denny to Address Data Privacy, GDPR and California Consumer Privacy Act of 2018 at Secure Delaware Workshop
October 31, 2018

Denny Presents on Managing Cybersecurity Risk, Cloud-Related Security and Data Breaches
September 27, 2018

Denny Presents on Cybersecurity Law at ABA Annual Meeting
August 2, 2018

Denny Moderates Panel on Data Privacy Basics for the Business Lawyer
May 31, 2018

Denny Delivers Keynote Address on Data Breach Disclosure Laws
May 22, 2018

Denny Presents on Data Breach Disclosure Laws, Creating Incident Response Plans
May 17, 2018

Denny and Reed Present at Data Security Workshop
May 2, 2018

Denny Discusses Best Practices for Mitigating Risks of Cyber Incidents
April 12, 2018

Denny Provides Update on Recent Amendment to Delaware’s Computer Security Breaches Law
March 1, 2018

Denny Moderates ABA Panel on Blockchain Technology and Smart Contracts
January 27, 2018

Denny Speaks on Panel Discussing Latest Issues Surrounding Cloud Security
December 6, 2017

Denny Addressed Cyber Security Trends and Best Practices at Secure Delaware Workshop
October 11, 2017

Denny Leads ABA Program on Vendor Risk and Cybersecurity Strategy
September 14, 2017

Denny Participates in Panel on Cyber Security Threats and Solutions
August 10, 2017
Potter Anderson Hosts Seminar on Protecting Your Business: Cyber Threats, Employees and Financial Security
May 16, 2017

2016 Secure Delaware Workshop
September 7, 2016

Protecting Your Business - Strategies for Growth and Resilience
February 23, 2016