Anton Collins Mitchell LLP
Accountants & Consultants

OCTOBER 2018
NATIONAL CYBER SECURITY AWARENESS MONTH

Written by Barbara Kaup, CPA, CGMA

In honor of National Cybersecurity Awareness Month, ACM would like to share a summary of new privacy revisions, Cyber updates in the New NAFTA and finally, thoughts around Due Diligence.

More than two-thirds (69%) of board directors have said their company is not impacted by the EU's GDPR. Chances are, many of them are wrong. More muted impact among corporate directors may reflect lack of awareness or misunderstanding that still underlies many aspects of this new regulation. Any U.S. company that deals with the personal data of EU citizens and residents could be subject to the GDPR's stringent requirements even if the company does not operate in any of the 28 EU member states.

Clearly, there is a lot of confusion about GDPR, not only because of its extraterritorial scope, but because of the ambiguity in the way it is written. It's not just GDPR, but many U.S. states and our other neighbors in North America, South America and Asia are moving forward with GDPR's or equivalents of their own.

Colorado

Effective September 1, 2018, Colorado enacted Privacy and Cybersecurity legislation, as part of the existing Consumer Protection Act:

Requires "covered entities" to implement and maintain reasonable security procedures, dispose of documents containing confidential information properly, ensure that confidential information is protected when transferred to third parties and notify affected individuals of data breaches.

Covered Entities	A person that maintains, owns or licenses personal identifying information in the course of the person's business, vocation or occupation.
Confidential Information/Personal Identifying Information (PII)	Social Security Number, Personal Identification Number, Password, Pass Code, Official State or government-issued driver's license or identification card number, government passport number, biometric data, employer, student or military identification number or financial transaction device.
Third-Party Requirements	Covered entities must take measures to protect PII when transferring it to third parties and require the third-party to implement and maintain reasonable security procedures and practices.
Document Formats	PII includes both electronic and paper documents and covered entities are required to develop a written policy for the destruction of such documents when they are no longer needed.

Key Highlights

Security Requirements:

- Implement and maintain reasonable security measures to protect PII;
- Contractually require third-party service providers to implement and maintain reasonable security measures through a vendor management program and include the 30-day requirement for breach notification;
- Implement a written policy to dispose of documents containing PII;
- Includes government agencies, but separated from Consumer Protection Act.

Breach Notification:

- 30-days to provide notice of a breach to affected individuals;
    - Shortest timeframe in the US with no exceptions;
    - No carve outs for HPPA and GLBA-regulated industries;
    - Law specifies what type of information must be included in the notice;
- Must report breach to Colorado Attorney General's office if breach notice sent to 500 or more Colorado residents;
- Must notify Credit Reporting agencies if breach notice sent to more than 1,000 residents;
- Personal information expanded to include a Colorado resident's first name or initial and last name in combination with any of the following:
    - Social Security number, student, military or passport identification number, driver's license number or identification card number, medical information, health insurance identification number or biometric data;
    - Username or email address in combination with a password or security questions and answers permitting access to an online account or a resident's account number;
    - Credit or debit card number in combination with any required security code, access code or password;
- No notice if data was encrypted, unless the encryption key was also compromised.

California

Two new laws are scheduled to take effect in California on January 1, 2020.

California Consumer Privacy Act (CCPA)

Introduced and passed legislation in seven days, only the data breach provision will be enforceable by the California Attorney General prior to July 1, 2020. All provisions are subject to interpretation by the Attorney General.

Who is Subject to CCPA?	For-profit business doing business in CA, plus: • Annual gross revenues >$25 million; • Personal information of >50,000 consumers, households or devices; • Sale of personal information accounts for >50% of annual revenue.
Exclusions	• HIPAA PHI Carve Out • Gramm-Leach personal information collections • Consumer Reporting Agency limited by the federal Fair Credit Reporting Act
Who is Covered?	Every individual domiciled in CA other than for a temporary or transitory purpose
What Information is Protected? (Individuals, Households and Devices)	• Biometric Data; • Geolocation Data; • Browse and Search History; • Purchase History; • Interactions with Ads and Apps; • Education Information; • Employment-related information; • Inferences drawn from the above information.
Additional Exclusions	• Government Information • Consolidated Information
Online Privacy Policy Requirements	• Describe Rights in online privacy notice; • List categories of Personal Information (PI); • Must update every 12 months; • Businesses that sell PI must have a "Do Not Sell My Personal Information" link on homepage.

Rights Provided:

- Right to Know up-front what personal information is being collected and with whom they are sharing. Entities must respond to verified requests to provide information to consumers;
- Right to be Forgotten subject to nine exceptions;
- Right to Opt Out of selling of consumer information to third parties for 12 months, then can approach consumer;
- Right to Opt In applicable to minors under 16 years of age. No one under 13 years of age;
- Right to Equal Service;
- Right to Data Portability.

The California Attorney General has the Right of Action to recover "not less than $100 and not greater than $750 – per consumer, per incident or actual damages, whichever is greater for nonencrypted or nonredacted PI data breach.

Internet of Things Law (IOT)

Any manufacturer of a connected device sold in California (yes, Alexa, Amazon Echo and Google Home, also televisions, security cameras, refrigerators and thermostats) that connects directly or indirectly to the internet through an Internet Protocol (IP) or Bluetooth address must equip it with reasonable security features designed to prevent unauthorized access, modification or information disclosure.

If it can be accessed outside a local area network with a password, it needs to either come with a unique password for each device or force users to set their own password the first time the device is connected.

Medical devices and other items subject to federal standards would be exempt.

GDPR and the California Laws

What now? What are the next steps and is the California CCPA the same as GDPR?

According to The Cyber Adviser Blog by Ballard Spahr, "CCPA is not a "mini-GDPR". GDPR contains 99 Articles, 173 recitals and is over 100 pages long whereas the CCPA is 16 pages long (approximately)."

Personal Information	Similar to GDPR with both addressing PI such as IP address and mobile devices
Processing	Similar and broad under both laws
Consumer	California residents vs. data subjects
Identification	California specifies "reasonably" identify from information. GDPR is similar, but does not include the reasonable qualifier

Business Entities	California: For-profit with three requirements with GDPR applying to both for-profit and nonprofit enterprises
Carve-Outs	California allows for public information not allowed by GDPR
Consumer Data	California includes specific requirement for website disclosures that address processing of personal information while both laws require specific disclosures addressing processing of personal information

While there are further similarities and differences between the two laws, CCPA will be emerging over the next year, plus as the California Attorney General defines its requirements.

Canada

Canada is Colorado's #1 customer and export market comprising exports of $1.4 billion and $3.6 billion of imports according to a 2017 Canadian government publication.

On April 18, 2018, the government of Canada published the final regulations relating to mandatory reporting of privacy breaches under Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). The regulations go into effect on November 1, 2018.

Within Canada	• Private sector organizations that collect, use or disclose personal information in the course of commercial activities; • Personal information about an employee of, or an applicant for, employment; • All personal information that flows across provincial or national boarders in the course of commercial transactions.
Outside Canada	• Foreign organizations with a real and substantial link to Canada – that collect, use or disclose the personal information of Canadians in the course of their commercial activities.

PIPEDA defines a "breach of security safeguards" and is similar to other breach notification statutes. The definition of "personal information" is extremely broad and defined as any information about an identifiable individual, including, but not limited to: name, age, ethnic origin, religion, social insurance number, email address, health information, financial information, biometric information, employee files, credit reports and education history.

Breach Notifications

Must notify individuals of any breach of the security of safeguards involving their personal information if it is reasonable to believe that the breach creates a "real risk of significant harm." Concurrently, the organization must also report to the Privacy Commission of Canada, with notices occurring "as soon as feasible" after the organization determines a breach has occurred.

PIPEDA specifies what must be included in the reports to individuals and the Privacy Commissioner with additional recordkeeping requirements for every breach for twenty-four months.

New NAFTA

The New NAFTA pact covers Data Privacy, Local Storage Rules and a Website Liability shield.

Data Privacy	• Data quality, Collection restrictions and transparency; • Governments will have to publish information on how businesses can comply with the New NAFTA rules and remedies by individuals.
Local Storage	• Bans rules requiring data to be stored locally; • Prohibits restrictions on data flows for business purposes.
Website Liability	Includes language similar to Section 230 of the Communications Decency Act: • Gives online publishers broad immunity for publishing, editing or removing third-party content; • Exception - Measures necessary to protect against online sex trafficking.

Cybersecurity and Due Diligence

Gardner predicts that by 2020, 60% of organizations engaging in mergers and acquisitions will consider the target company's cybersecurity posture as a critical factor in their due diligence process. Why it matters? Companies don't buy companies, they buy value – and their assets valued in an acquisition are the same ones that make it attractive to a hacker.

Based on an article published by Forbes, "concern about the accuracy, relevance and completeness of cybersecurity ratings has led the US Chamber of Commerce to publish a list of principles, supported by more than 40 organizations, including large banks and technology companies – for fair and accurate security ratings of companies."

About the Author

Barbara Kaup, CPA, CGMA

Senior Manager, Risk Advisory Services
Anton Collins Mitchell LLP
Direct: 720.795.9203
bkaup@acmllp.com