California Consumer Protection Act (CCPA) – What You Need to Know/Cyber Updates and the Role of Internal Audit

March 11, 2020
Introductions

BACKGROUND AND EXPERIENCE
E.J. Hilbert is the Managing Director of CNM’s Cyber and Privacy Services. E.J. has over 25 years of experience in the Security, Privacy, Risk Mitigation and Compliance fields. E.J.’s primary expertise is in helping clients establish a compliant Cyber Security strategy and then executing on that plan, often beginning with Cyber Security Awareness and Privacy training.

BACKGROUND AND EXPERIENCE
Justin Zavis is a Director with over 16 years of experience in Internal Audit, Regulatory Compliance, and consulting. Justin specializes in internal audit and regulatory compliance engagements within the financial services industry, and has experience in global banks, regional and community banks, investment management firms, and real estate. Justin leads CNM’s Los Angeles Financial Services Internal Audit Advisory practice.

BACKGROUND AND EXPERIENCE
Ernesto Carrasco is an IT Security Director in CNM’s Los Angeles office with 18 years of demonstrated success in operational strategies and information security risk management. His primary focus is the facilitation of privacy assessments (CCPA) information technology audits, incident handling, vulnerability, and penetration testing.
Learning Objectives

• Understand who CCPA covers and mandates under the law, including consumer data disclosure and data deletion

• Understand the impacts of non-compliance (penalties and liabilities) and periods of enforcement

• Understand current trends in the cyber security space

• Understand Internal Audit’s role around CCPA and cyber compliance
Question 1: Which of the following is an impact from CCPA?

a) Raises the cost of social media.

b) State Attorney General enforcement and civil penalties for non-compliance.

c) Prohibits the use and disclosure of consumer’s personal information.

d) Preempts all federal jurisdiction regarding privacy.

Correct Answer:
b) State Attorney General enforcement and civil penalties for non-compliance.
Gut Check cont.

**Question 2:** CCPA applies to companies that *only* have offices and employees in California.

**True or False?**

**Correct Answer:**
False. CCPA applies to businesses even if they have no physical presence in California.
Question 3: The CCPA applies to a business if it falls into one of the following buckets:

a) Annual gross revenue of $15,000,000 to $20,000,000.
b) Only buys, receives, sells or shares the personal information of households or devices for commercial purposes.
c) A not-for-profit entity that collects consumer personal data and has gross revenue of $25,000,000.
d) Derives 50% or more of its annual revenue from selling consumer personal information.

Correct Answer:
d) Derives 50% or more of its annual revenue from selling consumer personal information.
Why Does the Law Exist?

The intent of the Legislature is to further Californians’ right to privacy by giving consumers an effective way to control their personal information, by ensuring the following rights:

- The right of Californians to know what personal information is being collected about them.
- The right of Californians to access their personal information.
- The right of Californians to know whether their personal information is sold or disclosed, and to whom.
- The right of Californians to say no to the sale of personal information.
- The right of Californians to have equal service and price, even if they exercise their privacy rights.
The genesis of the California Consumer Privacy Act began with a ballot initiative by Alastair Mc Taggert. The timeline below details the evolution to where we are today:

- **October 12, 2017**: Ballot initiative by Alastair Mc Taggert was filed.
- **May 3, 2018**: Ballot initiative received 625,000 signatures.
- **June 21, 2018**: AB 375 was resurrected as “The California Consumer Right to Privacy Act of 2018”.
- **June 28, 2018**: California Consumer Privacy Act (CCPA) was signed into law.
- **August 31, 2018**: California State Legislature passes SB-1121.
- **October 11, 2019**: California Consumer Privacy Act (CCPA) Proposed Text of Regulations.
- **February 10, 2020**: Date for final comment submission.
- **December 6, 2019**: Modifications to Proposed Regulations.
- **January 1, 2020**: CCPA went live.
- **July 1, 2020**: CCPA went live.
Who is Covered by the Law?

For-profit businesses that collects personal information from CA residents that:

- Gross revenue is greater than $25 Million; or
- Derives 50% of annual revenue from sharing personal information; or
- Buys, sells, or shares personal information of 50,000 'consumers' or devices.

Note: CCPA applies to companies that may or may not have offices or employees in California, but that do “business in the State.”
According to the Franchise Tax Board, doing business in California consists of:

- Engaging in any transaction for the purpose of financial gain within California.
- Being organized or commercially domiciled in California.
- California sales, property, or payroll exceeding the following:
  - CA sales exceeding (either the threshold amount or 25% of total sales), or
  - CA real and tangible personal property exceeding (either the threshold amount or 25% of total sales), or
  - CA payroll compensation exceeding (either the threshold amount or 25% of total sales).

CCPA Impact to Consumers

The CCPA gives “consumers” four basic rights with regards to their personal information:

- **ACCESS**
  - “The Right to Know”

- **SALE**
  - The Right to “opt-out”

- **DELETION**
  - “The Right To Be Forgotten”

- **DISCRIMINATION**
  - The Right to “non-discrimination”
CCPA Impact to Businesses

The CCPA requires a business that collects a consumer’s personal information to maintain and manage the following:

01 Disclosure
- Anywhere that personal information is collected, companies must disclose consumers’ CCPA rights, and the categories of information collected and sold about them.

02 Consumer Requests
- Companies must put in place processes to comply with consumer requests to view and/or delete all information the organization has about them.

03 Opt-Out
- Companies are required to place a link titled “Do Not Sell My Personal Information” conspicuously on their homepage.

04 Auth. Minors
- The sale of children’s data will require express opt-in consent. If the child is between 13 and 16 years of age, express opt-in consent can be collected directly from the child. If the child is under 13 years of age, express opt-in consent will be required from the parental guardian.
What Kind of Information is Covered?

The CCPA Personal Information definition includes eleven specific categories, which are:

- Identifiers
- Internet Activity
- PI Categories CCR
- Geolocation Data
- Protected PI
- Olfactory Info
- Commercial Info
- Employment Info
- Biometric Info
- Education Info
- Inferences

[Note: The diagram includes a list of information categories such as Protected PI, Commercial Info, Biometric Info, Education Info, and Inferences, each represented by a different color and direction.]

California Customer Records statute (Cal. Civ. Code § 1798.80)e
What Kind of Information is Covered? (Cont.)

The CCPA deletion element does not apply to information that is subject to other federal regulations, including:

- The Health Insurance Portability and Accountability Act (HIPAA); the Gramm-Leach Bliley Act (GLBA);
- The Fair Credit Reporting Act (FCRA); or
- The Drivers’ Privacy Protection Act (DPPA).

The CCPA, however, will apply to entities covered by these laws to the extent they collect and process other personal information about consumers.
GDPR vs. CCPA

GDPR and CCPA differ in the following ways:

<table>
<thead>
<tr>
<th>GDPR</th>
<th>Definitions</th>
<th>CCPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>GDPR defines “personal data” to mean any information relating to an identified or identifiable data subject based on direct or indirect identification.</td>
<td><strong>Personal Information</strong></td>
<td>Broader definition includes “inferences,” “probabilistic identifiers” and shopping and browsing history</td>
</tr>
<tr>
<td>Fines of up to 4% of global revenue</td>
<td><strong>Fines</strong></td>
<td>Fines of up to $2,500 for each violation of the CCPA, or $7,500 per instance for intentional violations; violating entities subject to injunction</td>
</tr>
<tr>
<td>GDPR gives individuals a right to erasure when: Data is no longer necessary; the individual withdraws consent; the company has no legitimate interest; and unlawful processing</td>
<td><strong>Right To Be Forgotten</strong></td>
<td>Right to delete covers more types of information but has broader exceptions — the right to delete covers only data collected from the consumer (as opposed to access, which is broader)</td>
</tr>
<tr>
<td>GDPR gives individuals a right to object to the processing of PI in certain circumstances, and an absolute right to object to direct marketing</td>
<td><strong>Opt-Out</strong></td>
<td>CCPA provides a qualified opt-out right for the “selling” of personal information</td>
</tr>
</tbody>
</table>

Key Definitions

In order to comply with CCPA, certain definitions should be highlighted, including:

**Personal Information:**
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.

**Consumer:**
A natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.

**Service Provider:**
A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business.

**Third Party:**
Defined as any organization other than the first-party business that’s gathering data through consumer interaction, or service providers receiving consumer data from a company to fulfill its business goals.

**Selling Data:**
This includes a wide span of transactions involving the renting, transfer, or trade of private consumer data. Money doesn’t have to be exchanged, however; any compensation or benefit the seller receives may violate the CCPA’s terms if the data "sold" belongs to consumers who have opted out.

**Processing:**
"Processing" data under the CCPA refers to collection, possession, or other handling of data, whether manually or via automation; the data a consumer enters on a form is processed, just like that collected using cookies.
What is Required to Comply?

The process of preparing for compliance with the CCPA is going to take some work. Below are some key areas to address:

- Privacy Policy
- Request Processing
- Privacy Oversight
- Vendor Management
- Contract Review
- Training
- Parental Consent
- Reasonable Security
Enforcement and Penalties

Prior to action for statutory damages, the consumer must provide the Covered Business with 30 days to cure the alleged violation and to respond with a written statement that the violation has been cured.

• **Enforcement by Attorney General:**
  o For intentional violations, the CA Attorney General can seek penalties of up to $7,500 per violation.
  o For unintentional violations, the CA Attorney General can seek penalties of up to $2,500 if a business fails to cure the alleged violation within 30 days.

• **Private Enforcement Actions:**
  o Private plaintiffs can also bring an action for violations of the CCPA. For these private enforcement actions, the CCPA allows statutory damages from $100 to $750 per incident (or actual damages, whichever is greater).
Enforcement and Penalties (Cont.)

Here is a flow chart of the full CCPA private action procedure:

Question 1: How does CCPA define personal information?

a) Personal data or any information which is related to an identified or identifiable natural person. For example, the telephone, credit card or personnel number of a person, account data, license plate, appearance, customer number or address are all personal data.

b) 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.

c) Information that is capable of being associated with, or could be reasonably linked directly or indirectly, with a particular consumer or household.

d) Personal data which is related to an identified or identifiable natural person. For example, the telephone, credit card or personnel number of a person, account data, number plate, appearance, customer number or address are all personal data.

Correct Answer:
b) 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.
Question 2: If Facebook has approximately 24.6 million users in California and was found to have “intentionally” violated the CCPA, what would be an estimate of the maximum penalty?

a) $184.5 billion  
b) $55.4 billion  
c) $61.5 billion  
d) $65.7 billion

Correct Answer:  
a) $184.5 billion (approximately)
Question 3: What is the definition of “Reasonable Security”? 

a) A measuring tool to determine if consumer information was lost as a result of a data breach.

b) Breach of duty to investigate if consumer information was lost as a result of a data breach.

c) California residents should familiarize themselves with the CIS’s Top 20 Controls.

d) A measuring stick when determining if an organization’s behavior was a breach of a duty.

Correct Answer: 
d) A measuring stick when determining if an organization’s behavior was a breach of a duty.
How to Demonstrate Compliance

Below are areas that should be included within an organization’s Privacy Program:
Internal Audit Considerations

• Pre-implementation assessment – how did we do and are we ready?
  - Understand how management became comfortable that all compliance requirements were met (a crosswalk of requirement to internal controls/activities)
  - Review implementation plan (people, process, technology, training)
• Assess CCPA as part of your annual enterprise risk assessment.
  - Look at privacy and CCPA from a horizontal perspective across your organization
  - Consider results of pre-implantation reviews
  - Team up with management (first line) and compliance (second line)
  - Assess if there are thematic trends in review of privacy complaints
  - What were the results of privacy and CCPA training that was conducted at your organization
  - Assess operating effectiveness of internal controls
Internal Audit Considerations

• Pre-implementation assessment – how did we do and are we ready?
  - Understand how management became comfortable that all compliance requirements were met (a crosswalk of requirement to internal controls / activities)
  - Review implementation plan (people, process, technology, training)

• Post-implementation assessment – or full scope internal audit?
  - Through the annual enterprise risk assessment process, determine where your organization is overall with CCPA requirements. Would a full scope internal audit be value add? Or are there opportunities to conduct another current state or post-implementation assessment?
  - Conduct a risk assessment; consider reported incidents, training, and complaints to determine scope
  - Consider new processes implemented for streamlining opportunities
  - Execute – Assess operating effectiveness of internal controls
  - Report – Determine if there are thematic trends across your organization. What are your root causes of the thematic trends?
What We Expect

Once CCPA is fully established, we expect additional states to pass similar consumer privacy laws to the CCPA.

The highlighted states below already have proposed consumer privacy regulations:

- California: CCPA
- Hawaii: Consumer Privacy Protection Act
- Maryland: Consumer Privacy Protection Act
- New York: Data Privacy Act
- Massachusetts: Data Privacy Act
- Maine: Act to Protect Privacy
- Ohio: Data Protection Act
- Nevada: Consumer Privacy Law
- Hawaii: Consumer Privacy Protection Act
- Nevada: Consumer Privacy Law
CCPA Updates

On February 7th, 2020 changes were made to the proposed regulations. Below is a summary of the proposed regulations:

- § 999.305. Notice at Collection of Personal Information (a)(1) pg. 5 of 32; provide consumers with timely notice, at or before the time point of collection.
- § 999.305. Notice at Collection of Personal Information (a)(4) pg. 6 of 32; added guidance for collecting personal information from a mobile device.
- § 999.305. Notice at Collection of Personal Information (b)(4)(d) pg. 7 of 32; guidance for registered data brokers.
- § 999.312. Methods for Submitting Requests to Know and Requests to Delete (d) pg. 14 of 32; removed the two-step process for online requests to delete.
- § 999.314. Service Providers (a)(b)(c)(d)(e) pg. 19 of 32; Service provider changes.
- § 999.317. Training; Record-Keeping (g)(2)(3)(4) pg. 23 of 32; Disclosure of metrics information.
- § 999.330. Minors Under 13 Years of Age (c) pg. 29 of 32; Added bullet for documenting methods for determining whether a person submitting a request to know or a request to delete the personal information of a child under the age of 13 is the parent or guardian of that child.
CCPA Updates: Key Takeaways

• Comment solicitation closed on February 25th, 2020.
  ✓ 784 pages of comments were received and are currently being reviewed.
• The draft rules will be finalized sometime before July 1st, 2020.
  ✓ Given the number of comments, the CCPA effective date could be pushed to October 1.
• CCPA 2.0 ballot measure will be introduced in November 2020.
Cyber Updates

Top Three Cyber Threats for 2020, per the Federal Bureau of Investigation (FBI):

• Business Email Compromise
• Ransomware
• Advanced Persistent Threats
How can Internal Audit more effectively audit cyber risks within your organization?

- Detailed risk assessment and audit plan – going beyond the guidance that is set forth in publications such as the Federal Financial Institutions Examination Council (FFIEC) manual.
  - Be sure that testing plan includes:
    - Your organization’s configurations
    - Historical compliance
    - Complaints
    - Culture
    - Training and prior thematic issues
- Consider the use of advanced data analytics in your testing plan, if you have them available
- Internal Audit should have a seat at key steering committees where cyber risks are discussed
- Report
QUESTIONS?
LET'S PLAY A GAME!
CONTACT US

EJ Hilbert
Managing Director
T: 805-330-5894
E: ehilbert@cnmllp.com

Ernesto Carrasco
Director
T: 310-384-2003
E: ecarrasco@cnmllp.com

Justin Zavis
Director
T: 213.435.2041
E: jzavis@cnmllp.com

LOS ANGELES
A | 21051 Warner Center Lane
   Suite 140
   Woodland Hills, CA 91367
O | 818.999.9501
W | www.cnmllp.com

NEW YORK CITY
A | 300 Park Avenue
   Suite 12007
   New York, NY 10022

ORANGE COUNTY
A | 6 Venture
   Suite 365
   Irvine, CA 92618
O | 949.299.5582

SAN DIEGO
A | 8910 University Center Lane
   Suite 400
   San Diego, CA 92122