MINTZ

How Your Business Can Thrive Under The California Consumer Privacy Act

May 16, 2019

Moderator: Brian H. Lam

- Attorney in the Privacy and Data Security Practice
- Member of Governor's California Cyber Security Task Force
- Previously worked at Accenture in the Cybersecurity Advisory Practice, and Coalfire in the Cyber Risk Management and Compliance Practice
- Lots of Fun Acronyms:
  - Fellow of Information Privacy (FIP)
  - Certified Information Security Systems Professional (CISSP)
  - Certified Information Systems Manager (CIPM)
  - Certified Information Privacy Professional (CIPP)
  - M.S. Telecommunications Engineering
  - B.S. Computer Science

Panelist: Daniel T. Pascucci

- Member / Managing Member, San Diego Office; Co-chair, Class Action Practice
- Dan has served as lead defense counsel on over 70 alleged nationwide class actions, representing a variety of clients from Fortune 100 companies to smaller businesses in a diverse variety of industries, such as telecommunications carriers, technology manufacturers, retailers, investment services, banks, travel and recreation providers, and insurance companies.
- While the aggregate alleged exposure to his clients in class actions amounted to billions of dollars, no class has ever been certified over his objection, none of his class action clients has ever suffered an adverse judgment, and he has secured favorable settlements (often for no payment of cash or payment of minimal nuisance value) for his clients in all class actions he has defended.

Panelist: Evan Nadel

- Member / Co-chair, Class Action Practice
- Evan is a litigator who represents clients in disputes related to technology and handles the full gamut of class action cases. Evan’s work on technology-related and business disputes encompasses false advertising / unfair competition, trademark, licensing, privacy, and contract matters. He defends clients facing putative class actions around false advertising and product liability, including cases with California unfair competition and consumer protection law claims. Evan also has an active insurance litigation practice, handling coverage claims and disputes among primary and excess insurers in a variety of contexts.
- Evan Co-chairs the firm's Class Action practice group and his complex litigation practice is focused on technology-related litigation and class actions involving intellectual property, commercial contract disputes, along with insurance, trade secret, unfair competition, and other Internet-related litigation.

Panelist: Jason Mitchell

- Jason Mitchell is the General Counsel for Classy, Inc. a San Diego-based social enterprise that provides world-class online fundraising software to nonprofits.
- With extensive experience across general corporate law, intellectual property, and privacy, Jason's focus lies within negotiating and structuring transactions, including software and content licensing, outsourcing agreements, M&A/finance transactions, and general commercial agreements.
- Prior to Classy, Jason started his career as a corporate associate at Cahill Gordon & Reindel in New York City, and then worked in the General Counsels' offices of Moody's Investors Service and Active Network. Outside of work, Jason is an avid traveler, surfer, and judoka. Jason Received his BA, cum laude from the University of Pennsylvania and his JD, cum laude from NYU School of Law.

Panelist: Travis Stewart

- Senior Counsel at Lytx, Inc., one of the nation's leading video telematics and driver risk management companies, harnessing the power of data to change human behavior
- Assists various teams at Lytx with a diverse range of matters including compliance with privacy laws, data security, licensing and addressing the changing legal landscape of internet connected devices
- Prior to joining Lytx, Stewart was Corporate Counsel at FTD, Inc. (formerly, Provide Commerce, Inc.)

Covered in this Presentation

- Overview of CCPA
- CCPA Obligations by Entity Type
- CCPA Consumer Rights
- CCPA Litigation Risk Reduction Strategies
- CCPA Compliance Strategies

Overview of CCPA

Actions Covered by CCPA

- Provides rights to Consumers regarding their Personal Information as provided by CCPA.
- Understanding how CCPA applies will require understanding the information flow.
- The responsibilities imposed upon an entity, and what that entity will be able to do with personal information will depend on:

Whether the entity has Personal Information (as defined by CCPA).

Who the entity received the Personal Information from.

What rights the upstream provider of Personal Information (consumer or entity) has provided or denied, including through contract or opting out.

Many entities will have multiple data flows, and different corresponding rights and responsibilities as to each data flow.

Actions Covered By The CCPA: Who is a Consumer?

- A "**consumer**" is "a natural person who is a **California resident**, as defined in Section 17014 of Title 18 of the California Code of Regulations . . ., however identified, including by any unique identifier."
- Per these state regulations, a **California resident** is any individual who is (1) "in the state of California for other than a temporary or transitory purpose," or (2) "domiciled in the state" of California and "outside of the state for a temporary or transitory purpose."
- This is a broad definition. Note that a Consumer does not need to be engaging in a commercial activity to be a consumer.
- Personal Information originates from a Consumer. Understanding the data flow will require understanding who the Consumer is.

Overview of CCPA: Definition of Personal Information

- 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.”
- CCPA includes examples of Personal Information including: commercial information, including purchase histories, internet and network activity including search history, browsing history, interactions with apps, websites, or advertisements, geolocation data, profiles created from other Personal Information about a consumer.
- On August 31, 2018, via SB-1121, the California State Legislature made certain amendments to the CCPA. One of these was to clarify that these categories would only be Personal Information where they were linked or linkable to a consumer or household.
- Various bills may amend this definition including AB 873, AB 874 and AB 1355.
- Exclusions apply including certain information under HIPAA, GLBA, Driver’s Privacy Protection Act of 1994, and made “publicly available” that is “lawfully made available from federal, state, or local government records, if any conditions associated with such information.”

Overview of CCPA: Does Not Apply to Aggregate Consumer Information or Deidentified Data

- If data is “deidentified” such that it cannot be linked to a specific consumer, then it becomes “deidentified data” and CCPA does not apply.
- CCPA requires the use of technical safeguards and business processes to be used to prevent reidentification of this type of data.
- Similarly, CCPA does not apply to “aggregate consumer information” defined as “information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device.”
- When designing a business process or data flow, always consider whether deidentified or aggregate data could serve the business purpose.

Overview of CCPA: Collecting and Selling Personal Information

- Does Your Entity Collect Consumer Personal Information?
  - If your entity buys, gathers, rents, obtains, receives, or even accesses Consumer Personal Information, by any means, whether actively or passively, including by observing a Consumer's behavior, then it is collecting Consumer Personal Information.
- Is Your Entity Selling Personal Information?
  - Selling of Consumer Personal Information will occur where your entity is "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means [a Consumer's Personal Information]" for "monetary or other valuable consideration."
  - Note that "Selling" excludes for "use for a business purpose" where used by the business or a service provider for an operational purpose "reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed" or some other compatible operation purpose.
  - Seven specific business purposes are listed within CCPA.
  - These may change based on AB-1416, and SB-753.

CCPA Obligations by Entity Type

CCPA Entity Types – Understanding the Relationships Between the Three Entity Types

- CCPA imposes burdens on three different types of entities:
  - Businesses
  - Service Providers
  - Third Parties
- Much of the analysis has concerned what Businesses will need to do to comply, however it is important to consider what obligations may be imposed by the other two categories as well.
- A given entity could fall under all three categories, depending on its activities. Many entities will have more than one type of data flow subject to CCPA.
- Most Businesses will take advantage of one or more Service Providers.
- Many Service Providers may also be Businesses under CCPA because of employee information.

CCPA Entity Types: Is Your Entity a "Business" Under the CCPA?

- Are **each** of the following true?
  - Your entity **collects Personal Information from Consumers**, or another entity collects it for you.
  - **You determine**, or do so with others, **the purpose and reason for processing Consumer Personal Information**. Note this is a key distinction between Business and Service Providers. Service providers take their instructions from the Business.
  - **You do business in California**. While not defined by the CCPA, it is reasonably to assume that this would apply to any business who collects Personal Information from a Consumer. Thus, the Business does not need to be geographically located in California.
- Are **one or more** of the following true?
  - You have annual gross revenues in excess of $25,000,000.
  - You annually buy, share or receive for commercial purposes, or sell, the personal information of more than 50,000 consumers, including households and devices.
  - You receive 50 percent or more of your annual revenue from selling of consumers' personal information.

CCPA Entity Types: Is Your Entity a Service Provider Under the CCPA?

- Most every Business will use one or more Service Providers.
- **Service Providers** are entities 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**."
- The written contract must prevent the Service Provider from "from retaining, using, or disclosing personal information for any purpose," other than that of performing the services provided for by the contract.
- Further, Businesses must obligate their Service Providers to "direct any service providers to delete the consumer's personal information from their records" when a consumer requests that the Business do so.

CCPA Entity Types: Is Your Entity A Third Party Under the CCPA?

- CCPA describes what a “third party” is not.
- A “Third Party” is any entity that is not a CCPA Business, nor a Service Provider, but still receives a Consumer’s Personal Information from the Business.
- Consumers can only opt out of the providing of their Personal Information to Third Parties, not Service Providers.
- Third Parties cannot sell Personal Information about a Consumer sold to it by a Business unless the Consumer has been provided explicit notice regarding the opportunity to opt out of the sale.

CCPA Consumer Rights

CCPA Consumer Rights: Overview

- The CCPA provides dramatic changes to the rights granted to Consumers.
- Businesses need to support the following rights:
  - Disclosure/Privacy Policy Requirements
  - Access/Data Portability
  - Deletion
  - Opt Out Requirements/Non-discrimination
- These rights apply to all Personal Information collected from Consumers by a Business.
- Service Providers will need to be able to support these rights.
- Businesses need to be able to ensure their processes and contracts will enable them to meet these requirements.
- Third Parties will want to protect themselves via contract and due diligence as to any data they receive.

CCPA Consumer Rights: Disclosure/Privacy Policy Requirements

- Before or at the time of collection, a Business must:
  - Inform Consumers of the categories of Personal Information to be collected.
  - Inform Consumers of the purposes for which the categories of Personal Information shall be used.
  - Provide notice of the collection of any additional categories of information or use of collected information for any additional purposes taking place after initial disclosures have been made.
- Privacy Policy Requirements
  - A listing of Consumers' rights under the CCPA, including the consumer right to opt out of the sale of the Consumer's Personal Information and a separate link to the "Do Not Sell My Personal Information" on the Business's website.
  - How Consumers may submit requests to exercise their rights to the Business.
  - A list of the categories of Personal Information that the Business has collected about Consumers, sold about Consumers, and disclosed about Consumers for a business purpose in the preceding 12 months.

CCPA Consumer Rights: Access/Data Portability

- Upon a Verifiable Consumer Request No More Than Twice Per Year
  - Businesses That Collect Personal Information About the Consumer Must Provide:
    - Categories, sources, and business or commercial purpose for collecting of Personal Information the Business has collected about the Consumer
    - Categories of third parties with which the business shares Personal Information
    - Disclose and **provide specific pieces** of Personal Information the Business has collected about the Consumer.
    - Business must provide Personal Information in "readily usable format" that allows porting the data over to another entity "without hindrance."
    - Businesses are not required to retain information that is obtained in a one-time transaction or to re-identify or link information that is not in identifiable form.
  - Businesses That Sell Personal Information About the Consumer Must Provide:
    - Categories of Personal Information the Business has collected about the Consumer
    - Categories of Personal Information the Business has sold about the Consumer
    - Categories of Third Parties that the Personal Information was sold by category or categories of Personal Information for each third party to which the personal information was sold
    - Categories of personal information the Business has disclosed about the Consumer for a business purpose

CCPA Consumer Rights: Deletion

- Can request deletion of Personal Information (from Business and its Service Providers)
- The CCPA provides that Consumers can request that a Business delete **any** Personal Information about the Consumer, so it may be that Consumers can request partial deletions.
- Many exceptions are present.
  - Necessary to provide a good or service requested by the Consumer or reasonably anticipated due to relationship with the Consumer.
  - Detecting security incidents or fraud, as well as debugging existing intended systems.
  - Enabling internal uses that are aligned with Consumer expectations based on the relationship.
  - Complying with legal obligations.
  - These exceptions could be construed to be fairly broad in nature, particularly as they relate to detecting fraud, and debugging systems.

CCPA Consumer Rights: Opt Out Requirements/ Non-Discrimination

Opt Out	The CCPA authorizes a Consumer to opt out of the sale of Personal Information by a Business. Businesses must make available, in a form reasonably accessible to Consumers, a "clear and conspicuous link to the homepage", titled "Do Not Sell My Personal Information." That link must go to a webpage that enables the Consumer to opt out. The Business must wait a minimum of 12 months before requesting to sell the Personal Information of a Consumer who has opted out.
Non-Discrimination	Businesses are prohibited from discriminating against the Consumer for exercising this right, including by charging the Consumer who opts out a different price or providing the Consumer a different quality of goods or services, except if the difference is reasonably related to value provided by the Consumer's data. Financial incentives offered to the Consumer for the collection, sale, or deletion of Personal Information are permitted only with the prior opt in by the Consumer.

CCPA Litigation Risk Reduction Strategies

Two litigation risks:

1. Attorney General Action against businesses that collect personal information for violation of the Act's provisions.
2. Private right of action:
    a. By any consumer
    b. whose nonencrypted or nonredacted personal information
    c. is subject to an unauthorized access and exfiltration, theft or disclosure
    d. as a result of the business's violation of the duty to implement and maintain reasonable security procedures

CCPA Class Action Damages

- Damages measured as ***greater of***:
  - actual damages, ***or***
  - statutory damages of $100 to $750 per consumer per incident

Balance Sheet Discovery

“In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant’s misconduct, and the defendant’s assets, liabilities, and net worth.”

Safe-Harbor Provision

30-day safe-harbor provision provides limited relief:

- Similar to CLRA Provision, which has not prevented surge of CLRA suits;
- Written statement requirement creates further liability exposure:
  - Consumer may sue to enforce written statement;
  - May pursue statutory damages for each breach of the written statement ***in addition to*** other violations of the Act;
- Cure may not be available in data breach cases
- Not required if suing only for actual pecuniary damages

Is Help On the Way?

- SB-561 is in committee:
  - Would allow private action for any violations of the act, giving consumers the same scope as the AG
  - Would remove 30-day notice and cure provision from AG actions, but not consumer actions
- Likely to see constitutional challenges to the statute:
  - Statutory damages are not tethered to reality
  - Consideration of balance sheet of defendant in calculating damages is punitive without showing of malice, oppression or fraud
  - Possible First Amendment, Commerce Clause and ambiguity challenges
  - These challenges can be raised in an industry-backed lawsuit or used as defenses

Self Help

- Bullet-proofing compliance to ensure that any breach is not caused by lack of reasonable safety procedures:
  - ISO 27002 Compliance
  - Implementation of the 20 CIS Controls
    - Recommended by CA AG in 2016 *California Data Breach Report*
- Adopt and implement strong arbitration clause compliant with *AT&T v. Concepcion*
  - Customize to situation to ensure enforceability; ie, don't use a stock clause
  - Include language agreeing to bilateral arbitration, waiving class action rights and delegating determination of arbitrability to arbitrator.
  - Arbitration agreements are NOT just for online services (via TOS or terms and conditions) – "brick and mortar" companies have options for proposing arbitration agreements too

Class Action Mitigation Strategies

- Patchwork of Counter-Measures and Policies:
  - Use IP address and/or drop down menus to determine state of residency – different path for CA users online
  - Loyalty program/affinity club and/or company-sponsored credit card – include bilateral arbitration agreement for members/users for all transactions, even when not using that card
  - Mobile app has arbitration agreement in terms and conditions applicable to all transactions between customer and company
  - Point of sale touchscreen – including consent to bilateral arbitration, with paper copy of full agreement at register and follow-up email sending full terms

Class Action Mitigation Strategies (cont'd)

- Include disclosures and policies on 30-day cure period – for example, customer agrees to accept the greater of individual actual damages substantiated by customer or $100 in the event of data breach, in addition to change in company policies to address any data security weakness exposed by breach if reasonable and appropriate.
- Change policies every year or more often to update with new technology (e.g. encryption)
- Agreements with vendors and partners re protection and availability of individual user "personal information" to facilitate compliance with CCPA

CCPA Compliance Strategies

CCPA Compliance Strategies

- Understand how Personal Information flows through your organization.
- **Points of Collection**: Have privacy policies or other mechanisms been updated to disclose what information is being collected, disclosed, and sold? Does the privacy policy provide a disclosure of the right to opt-out of any such selling? Does it explain the new Consumer rights provided by the CCPA?
- **Data Management**: Complying with the CCPA will require understanding where Personal Information is at any given time. Companies will need mechanisms to track business processes, products, devices, applications and third parties that access the Personal Information of Consumers.
- **Support for Consumer CCPA Rights**: The rights of Access/Data Portability, Deletion, Opt Out Requirements/Non-discrimination will require support throughout the organization, and at the information technology infrastructure level.
  - **Consumer Requests**: Verify, document and support requests.
  - **Create Systems of Record**: This will serve as a record of the execution of Consumer requests.
  - **Provide Training**: Stakeholders must be informed and empowered to act.
  - **Testing**: Test processes and controls before January, 2020.

CCPA Compliance Strategies

- **Information Security**: Identify and close any security gaps.
  - The CCPA will greatly increase the cost of non-remediated gaps through its statutory damages provision within the private right of action.
  - Being able to track where data was, and attest that it was not breached will be important for limiting exposure.
- **Service Provider Agreements**: Create a process for reviewing current and future contracts and negotiating necessary CCPA amendments. Remember that if appropriate provisions are not in place, there is the possibility that the vendor may not be considered a Service Provider under the CCPA.
  - Service Provider must refrain "from retaining, using, or disclosing personal information for any purpose," other than that of performing the services provided for by the contract.
  - Service Provider must agree to support Consumer CCPA rights, including Access/Portability, Deletion, and Opt-outs.

CCPA Compliance Strategies

- **Business Model Analysis**: Consider whether any portion of the CCPA would motivate the redesign of a business process or external offering.
  - How will the antidiscrimination provisions be dealt with?
  - How will the Business calculate the value provided by the Consumer's data?
  - How would the offering of financial incentives to the Consumer for the collection or sale of Personal Information impact the viability of the Business?
- **Achieve Corporate Buy-In**
  - Culturally, how does the Business plan to make CCPA compliance a priority while demonstrating its value to stakeholders?
  - Can the Business use its newly created CCPA processes as a competitive advantage?

MINTZ

THANK YOU

Check out our blog: https://www.privacyandsecuritymatters.com/

Dan Pascucci

Managing Member, San Diego Office; Co-chair, Class Action Practice

San Diego

DPascucci@mintz.com +1.858.314.1505

Evan Nadel

Member / Co-chair, Class Action Practice

San Francisco

Enadel@mintz.com +1.415.432.6016

Brian Lam

Attorney

San Diego

BHLam@mintz.com +1.858.314.1583