Drinker Biddle®

California Consumer Privacy Act Overview

The California Consumer Privacy Act of 2018 ("CCPA" or "the Act") takes effect on January 1, 2020.

KEY DEFINITIONS

Despite its name, the CCPA applies to a broader class of individuals than colloquial understandings of "consumers." The term "consumer" is defined under the Act, in relevant part, as "a natural person who is a California resident." Thus, customers, employees, business contacts, and others are protected individuals under the Act.

"Personal Information" is broadly defined under the CCPA and includes a number of enumerated categories of personal information. In general, information that can be linked to a person, device, or browser will be considered "personal information."

KEY REQUIREMENTS

The CCPA empowers CA residents with the following six data privacy rights:

1. To be provided with information on what personal information is collected about them and the purposes for which that personal information is used.
2. To be provided with information on what personal information is sold or disclosed for a business purpose and to whom.
3. To opt out of the sale of their personal information to third parties (or in the case of minors under age 16, to require an opt in before the sale of their personal information).
4. To request the deletion of their personal information.
5. Not to be subject to discrimination for exercising any of the above rights, including being denied goods or services or being charged a different price, or being subjected to a lower level of quality, of such goods or services.
6. To seek statutory damages of $100 to $750 for breaches of unencrypted personal information that arise as a result of a business' violation of its duty to implement and maintain reasonable security procedures.

The CCPA also requires that a business must in its online privacy policy, or in a California-specific privacy policy posted on its website, describe CA residents' rights to request information and list the categories of CA residents' personal information it has in the prior 12 months (i) collected, (ii) sold, and (iii) disclosed for business operational purposes.

In addition to describing the right to opt-out in its online privacy policy or California-specific privacy policy, a business must include a "clear and conspicuous" link on its homepage to a web page where individuals can exercise their opt out rights. The link must be titled "Do Not Sell My Personal Information" and must link to a page with the same title.

Contracting for CCPA Compliance

Presenters:
Jeremiah Posedel
jeremiah.posedel@dbr.com

Reed Abrahamson
reed.abrahamson@dbr.com

CCPA Webinar #5
July 17, 2019

Drinker Biddle

Webinar Schedule

1:00 – 2:00 PM US Eastern

- Today
- August 21, 2019
- September 25, 2019
- October 30, 2019
- December 4, 2019

Let us know what topics you would like us to focus on in the upcoming webinars!

CCPA 2020

Agenda

- Compliance Roles & Key Terms
- Business > Service Provider Agreements
- Business > Third Party Agreements
- General Contracting Terms
- Questions

Compliance Roles & Key Terms

Compliance Roles

- Under the CCPA, compliance obligations attach to three different types of entities:
  - a "business"
  - a "service provider"
  - a "third party"
- Compliance obligations and associated contracting requirements depend on party's role.

”Business”

“Business” means a for-profit entity that collects consumers' personal information, or on the behalf of which such information is collected, and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:

- Has annual gross revenues in excess of twenty-five million dollars ($25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.
- Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.
- Derives 50 percent or more of its annual revenues from selling consumers' personal information.

- Business includes any entity that controls or is controlled by a business, as defined above, and that shares common branding with the business.

CCPA 2020

”Service Provider”

“Service provider” means a for-profit 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*, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by the CCPA, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.”

"Third Party"

"Third party" means a person who is not any of the following:

- The business that collects personal information from consumers under the CCPA.
- A person to whom the business discloses a consumer's personal information for a **business purpose** *pursuant to a written contract*, provided that the contract both:
  - Prohibits the person receiving the personal information from:
    - **Selling the personal information**.
    - Retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract.
    - **Retaining, using, or disclosing the information outside of the direct business relationship between the person and the business**.
  - Includes a certification made by the person receiving the personal information that the person understands the restrictions above and will comply with them.

CCPA 2020

Service Provider v. Third Party

- The third party definition adds prohibitions that must be included within the written contract between the business and the service provider in order for the service provider to not be considered a third party:
  - Prohibition on selling personal information.
  - A certification made by the service provider (or other person) receiving the personal information that they understand the restrictions and will comply with them.

CCPA 2020

Service Provider v. Third Party

Why do these additional contract provisions matter?

- If the service provider is considered a third party, the business has additional obligations:
  - Notice to consumers must identify the categories of third parties to who information is shared. [179.110]
  - Business must disclose the categories of third parties to whom personal information was sold and categories of third parties to whom personal information was disclosed for a business purpose. [179.115/130]
  - "Selling" definition and provisions apply to sales to third parties or other businesses.

Other Key Terms: "Business Purpose"

"**Business purpose**" means the use of personal information for the business's or a service provider's operational purposes, or other notified purposes, provided that the use of personal information shall be *reasonably necessary and proportionate* to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected.

CCPA 2020

Other Key Terms: "Business Purpose"

"**Business purposes**" are:

- Auditing related to a current interaction with the consumer and concurrent transactions, including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.
- Detecting security incidents, protecting against malicious/illegal activity, and prosecuting those responsible.
- Debugging to identify and repair errors.
- Short-term, transient use, provided the personal information that is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer's experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction.
- Performing services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider.
- Undertaking internal research for technological development and demonstration.
- Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

Other Key Terms: "Sell"

"Sell," "selling," "sale," or "sold," means 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 *by the business* to another business or a third party for **monetary or other valuable consideration**.

CCPA 2020

Other Key Terms: Not "Selling"

A business does not sell personal information when:

- A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of the CCPA.
- The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's personal information for the purposes of alerting third parties that the consumer has opted out of the sale of the consumer's personal information.
- The business uses or shares with a service provider personal information of a consumer that is necessary to perform a **business purpose** if both of the following conditions are met:
  - The business has provided notice that information being used or shared in its terms and conditions.
  - The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.

Other Key Terms: Not "Selling"

A business does not sell personal information when:

- The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with Sections 1798.110 and 1798.115.
  - If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer.
  - This foregoing provision does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy.

CCPA 2020

Business > Service Provider Agreements

Written contract between the business and service provider (1)

- The contract should state which party is the "service provider" and that the such party receives and processes the personal information from and on behalf of the business pursuant to a **business purpose**.
  - *It is unclear whether it is necessary to state the specific business purpose. However, until further guidance is issued, applicable purposes should be included in the contract where possible to mitigate compliance risk*.

Written contract between the business and service provider (2)

- Prohibit the service provider from "retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract."
- Prohibit the service provider from "retaining, using, or disclosing the information outside of the direct business relationship between the service provider and the business."
- Prohibit the service provider from selling the personal information (*as "sell" is defined under the CCPA*).
- Include a certification made by the service provider that the service provider understands the restrictions above and will comply with them.

Written contract between the business and service provider (3)

- When the business uses or shares personal information with the service provider, the contract should prohibit the service provider from further collecting, selling, or using the personal information except as necessary to perform the business purpose.
- The service provider should provide all necessary assistance to the business to allow the business to comply with its CCPA obligations, including providing the business with any information needed to respond to a consumer's request to exercise rights under the CCPA.
- Upon request by the business, the service provider must permanently delete personal information about a consumer.
- Upon request by the business, service provider must immediately cease any sale of a consumer's personal information.
- If service provider receives any requests from a consumer related to personal information service provider processes for the purpose of fulfilling obligations to the business, service provider should inform the business of the request [within 5 business days] and take the actions directed by the business to respond to the request within the time period provided by the CCPA.
- Service provider should implement all reasonable and appropriate security measures to protect personal information.
  - *The business may require service provider to implement all Center for Information Security Critical Security Controls and any applicable security measures recommended by the California Attorney General's Office.*

Business > Third Party Agreements

Contract between the business and third party

- If a business sells personal information to a third party, the contract should prohibit the third party from also selling the personal information unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to Section 1798.120.

Contract between the business and third party (No Sale)

- When a consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, the contract between the business and the third party should prohibit the third party from also selling the personal information (unless that disclosure would be consistent with the provisions of the CCPA).
  - Otherwise, the disclosure from the business to the third party may constitute a sale of personal information.

General Terms

General Terms

- Define key terms using CCPA definitions:
  - “Sell”
  - “Personal Information”
  - “Deidentified”
- Explicitly require compliance with the CCPA
- Indemnification
  - Address statutory damages.
- Limitation of Liability
- Change in Law

Questions?

DrinkerBiddle®

Jeremiah Posedel

Associate | Chicago

jeremiah.posedel@dbr.com
Phone: (312) 569-1504

About

Jeremiah Posedel is a member of Drinker Biddle's Information Privacy, Security and Governance team and Information Technology and Outsourcing team. Jeremiah's practice is at the interface of law, technology and privacy, integrating two distinct but overlapping domains: information technology transactions and data privacy and security.

First, Jeremiah advises on and negotiates a wide array of transactions involving the acquisition, development, leveraging and marketing of information technology assets, including hardware, software and database licensing, outsourcing and cloud-based services arrangements, and system implementation and support agreements.

Second, Jeremiah counsels clients on domestic and international privacy and security regulations and standards applicable to the collection, use and disclosure of personal data, including the FTC Act, GLBA, FCRA, HIPAA, COPPA, CAN-SPAM, TCPA, California Consumer Privacy Act (CCPA), NAIC model regulations and guidance, PCI DSS, DAA Program for Online Behavioral Advertising, and EU General Data Protection Regulation. He works with organizations to develop and implement comprehensive privacy/security programs and compliance strategies focused on a variety of data processing activities, including digital and interest-based advertising, big data analytics and profiling, blockchain deployment, workplace monitoring, mobile device and app deployment, cross-border data transfers, and InsurTech and e-commerce initiatives.

Jeremiah is a Certified Information Privacy Professional (US/Europe/Canada) and a visiting Lecturer of Law (information privacy) at Bucerius Law School in Hamburg, Germany. In 2004, Jeremiah served as a deputy campaign director to President Barack Obama's successful U.S. Senate campaign.

Areas of Focus

Services

- Information Technology and Outsourcing
- Intellectual Property
- International
- Technology Transactions and Licensing
- Information Privacy
- Information Security

Industries

- Health Care
- Pharma and Life Sciences
- Retail
- Insurance
- InsurTech
- Technology

Credentials

Bar Admissions

- Illinois

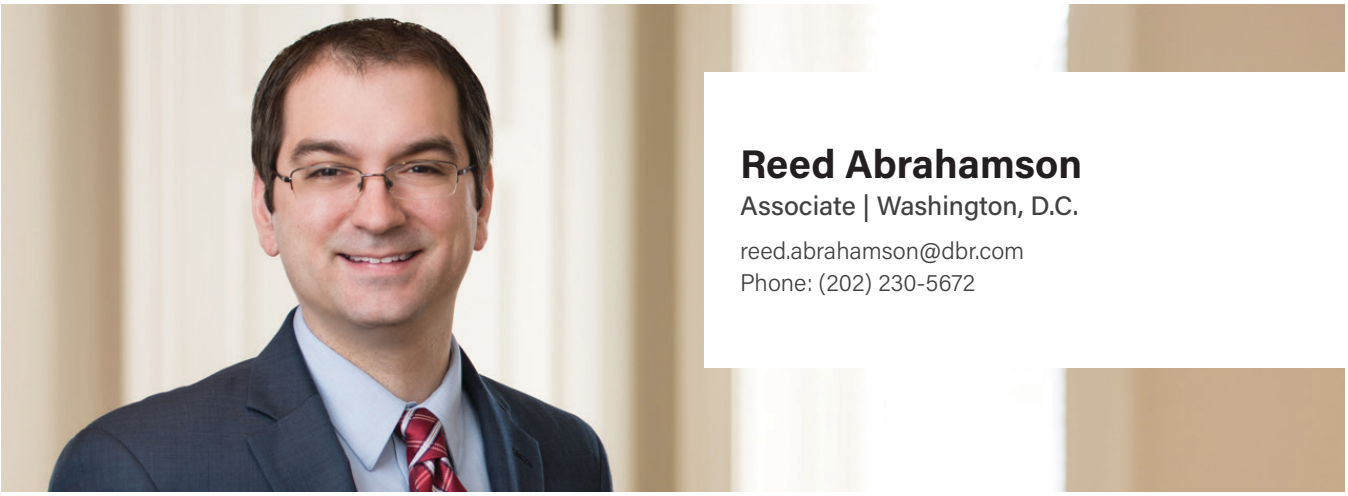
Court Admissions

- U.S. District Court, Central District of Illinois
- U.S. District Court, Northern District of Illinois

Education

- University of Illinois College of Law, J.D., 2006, *cum laude*
- Bucerius Law School, Hamburg Germany, 2006
- Valparaiso University, B.A., 2000, *cum laude*

DrinkerBiddle®



Reed Abrahamson

Associate | Washington, D.C.

reed.abrahamson@dbr.com
Phone: (202) 230-5672

About

Reed Abrahamson assists clients with identifying and addressing data privacy and security risks in business operations. He has helped companies design and implement privacy and data security policies and programs, and advises clients on compliance issues related to HIPAA, CAN-SPAM Act, TCPA, and other privacy laws. Reed also has experience working with companies to respond to data breach incidents.

A United States Certified Information Privacy Professional (CIPP-US), Reed works with in-house teams to create frameworks for international transfers of regulated personal information, particularly from the European Union to the United States.

Reed also counsels clients on managing risk through appropriate policies and contractual arrangements, including drafting and modifying customer and consumer-facing privacy policies and statements. He has helped clients retain service providers and enter into arrangements with customers.

In addition, as a member of the firm's Consortia Management Team, Reed works on the formation, management, and representation of consortia in the life sciences industry that address matters of science, policy, law, and business operations. He assists in the creation of appropriate collaboration mechanisms and provides legal support for the day-to-day activities of these organizations.

Reed served as a law clerk to the senior judges for the District of Columbia Court of Appeals.

Areas of Focus

Services

- Consortia Management
- Government and Regulatory Affairs
- Information Privacy, Security and Governance
- Technology Transactions and Licensing

Industries

- Pharma and Life Sciences

Credentials

Bar Admissions

- District of Columbia
- Maryland

Education

- Georgetown University Law Center, J.D., 2012, *magna cum laude, Georgetown Immigration Law Journal*
- Yale University, B.A., 2008