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.

# What Does It Mean? – A Discussion of CCPA's Thorny Interpretation Issues


***Presenters:***

**Katherine Armstrong**
*katherine.armstrong@dbr.com*

**Peter Blenkinsop**
*peter.blenkinsop@dbr.com*

**Jeremiah Posedel**
*jeremiah.posedel@dbr.com*


***CCPA Webinar #4***
***June 12, 2019***

Drinker Biddle

# Webinar Schedule

***1:00 – 2:00 PM US Eastern***

- Today
- July 17, 2019
- 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!**

# Agenda

- Update on Legislative Amendments
- Interpretation / Implementation Issues


# Update on Legislative Amendments

# Legislative Amendments

- Outline Process and Timeline
- Review Significant Bills

# California – AB 25

- *Status: Passed Assembly; awaiting Senate committee assignment*
- Adds the following exclusion from definition of a "consumer":
  - “ 'Consumer' does not include a natural person whose personal information has been collected by a business in the course of a person acting as a job applicant or as an employee, contractor, or agent, on behalf of the business, to the extent their personal information is used for purposes compatible with the context of the person’s activities for the business as a job applicant, employee, contractor, or agent of the business.“

# California – AB 873

- *Status: Passed Assembly; in Senate Judiciary*
- Seeks to clarify definitions of "personal information" and of "de-identified information“
  - “Personal information” would mean information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:....
  - (h) “Deidentified” means information that ~~cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked,~~ does not identify and is not reasonably linkable, directly or indirectly, to a particular consumer, provided that ~~a business that uses deidentified information:~~ the business makes no attempt to reidentify the information, and takes reasonable technical and administrative measures designed to:

    (1) ~~Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.~~ Ensure that the data is deidentified.

    (2) ~~Has implemented business processes that specifically prohibit reidentification of the information.~~ Publicly commit to maintain and use the data in a deidentified form.

    ~~(3) Has implemented business processes to prevent inadvertent release of deidentified information.~~

    ~~(4)~~ (3) ~~Makes no attempt~~ Contractually prohibit recipients of the data from trying to reidentify the information. data.

CCPA 2020

# California – AB 874

- *Status: Passed Assembly; in Senate Judiciary*
- Seeks to clarify public record exception to definition of "personal information."
  - "Publicly available" would mean information that is lawfully made available from federal, state, or local records.
- Provides that "personal information" does not include consumer information that is deidentified or aggregate consumer information.

# California – AB 1355

- *Status: Passed Assembly; in Senate Judiciary*
- Seeks to clarify certain ambiguities and/or drafting errors, including related to content of notice at point of collection and exemption related to offering financial incentives.
  - Notice must include: That a consumer has *the right to request* the specific pieces of personal information the business has collected about that consumer.
  - A consumer has the right to request information on: The categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each ~~third party~~ category of third parties to whom the personal information was sold.
  - With respect to non-discrimination provision: Nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer business by the consumer's data.

# California – AB 846

- *Status: Passed Assembly; in Senate Judiciary*
- Clarifies that the CCPA does not prohibit a consumer from choosing to participate in customer loyalty programs
- ***New 1798.126.***

  *(a) This title shall not be construed to prohibit a business from offering a different price, rate, level, or quality of goods or services to a consumer, including offering its goods or services for no fee, if either of the following is true:*

  *(1) The offering is in connection with a consumer's voluntary participation in a loyalty, rewards, premium features, discounts, or club card program.*

  *(2) The offering is for a specific good or service whose functionality is directly related to the collection, use, or sale of the consumer's data.*

  *(b) A business shall not offer loyalty, rewards, premium features, discounts, or club card programs that are unjust, unreasonable, coercive, or usurious in nature.*

  *(c) As used in this section, "loyalty, rewards, premium features, discounts, or club card program" includes an offering to one or more consumers of lower prices or rates for goods or services or a higher level or quality of goods or services, including through the use of discounts or other benefits, or a program through which consumers earn points, rewards, credits, incentives, gift cards or certificates, coupons, or access to sales or discounts on a priority or exclusive basis.*

# California – AB 1416

- Status: *Passed Assembly; awaiting Senate committee assignment*
- Clarifies that the CCPA does not prohibit businesses from providing a consumer's personal information to a government agency in order to comply with rules and regulations.

# California – AB 1564

- Status: *Passed Assembly; in Senate Judiciary*
- Seeks to provide alternative to current CCPA requirement that businesses must establish a toll-free number to receive CCPA requests.

  1798.130(a)...

  (1) (A) Make available to consumers ~~two or more designated methods~~ a toll-free telephone number or an email address and a physical address for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and ~~1798.115, including, at a minimum, a toll-free telephone number, and if the business maintains an Internet Web site, a Web site address.~~ 1798.115. A business that operates exclusively online shall only be required to provide an email address for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115.

  (B) If the business maintains an internet website, make the internet website available to consumers to submit requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115.


# Interpretation / Implementation Issues

# Definition and Scope of Consumer

- Consumer
  - Who is a California resident?
  - Does it include business contacts?

# Definition and Scope of Personal Information

- Includes the following "if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household":
  - Audio, electronic, visual, thermal, olfactory, or similar information
  - Internet or other electronic network activity information, such as browsing and search history
  - Inferences used to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence abilities, or aptitudes

# Personal Information

- What are the limits of personal information
  - 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.”
  - What is a “particular consumer”?
  - What does “relates to [or] describes” mean?
  - What is reasonably linked directly or indirectly?
  - How to handle “household” data?
  - What standard for de-identified/anonymized data?

# Mechanics for Consumers to Exercise Rights

- Requirement:  Make available to consumers two or more designated methods for submitting requests including, at a minimum, a toll-free telephone number, and if the business maintains an Internet Web site, a Web site address
- Toll-free number
  - Is IVR allowed?
- Timing for requests
  - 45 days just for access?
  - What is response time for deletion and do not sell requests?
- What internal tracking is needed to demonstrate process is timely and responsive?

# Notice

- Requirement:  At or before time of collection and on website
- At time of collection
  - Online, telephone inquiries, retail stores …
- Website
  - Provide California-only notice?
  - Blended US notice
  - How does “Do Not Sell My Personal Information” link work?

# Verifiable Requests

- Waiting for regulations
- What is appropriate level of authentication for each category of consumer?
  - How to authenticate a website visitor?
- Does it vary upon request?
  - Access – risk of private right of action if given to wrong person
  - Do not sell
  - Delete
- Process for handling disputes

# Access

- Requirement:  In response to a verifiable consumer request, a business must disclose the personal information it has collected about the consumer
- What is look back period, January 1, 2019 or January 1, 2020?
- Is there a duty to preserve data once request is made?

# Access

- What is provided?
  - Categories of data collected
  - Business purpose
  - Categories of data sold and to whom sold
  - Specific pieces of information
    - All data from every database? Or main database?

# Definition of Sale

- "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."
  - What are examples of communicating orally?
  - What is other valuable consideration?

# Do Not Sell

- What is a sale?
  - Transfers to affiliates?
  - Transfers to website partners?
  - How to handle ad tech space?
- What is not a sale?
  - At the direction of the consumer
    - Is that a waiver of rights?
  - Transfer to service providers
    - What is required in contracts with service providers and/or other service provider certifications?

# Do Not Sell

- Where does Do Not Sell button need to be placed?
- What is timing for responding to requests?
- How often can requests be made?
- What does response to consumer include?
- How to track requests?

# Delete data

- Requirement: “Delete any personal information about the consumer which the business has collected from the consumer.” “Must delete personal information from its records and direct any service providers to delete the consumer’s personal information.”

# Request to Delete Data

- What is timing for responding to request?
- How often can requests be made?
- How to handle deletion of some, but not all data?
- How to verify action taken internally and with service providers?
- Is there a continuing obligation to delete data?

# Distinguishing Financial Incentives from Discrimination

- Prohibition:  A business may not charge consumers more or offer reduced services if the consumer exercises their rights.  However, a business may offer certain financial incentives to consumers or adjust pricing or service levels based on the value of the consumer's data to the consumer"

# Non-Discrimination

- How to demonstrate that financial incentives are not discriminatory?
- How to reconcile prohibition with ability to request consumer to authorize the sale of their data 12 months after opting out?
- How does this work with loyalty programs?


# Questions?

DrinkerBiddle®


# Katherine E. Armstrong

Counsel | Washington, D.C.

katherine.armstrong@dbr.com
Phone: (202) 230-5674


## About

**Katherine E. Armstrong** assists clients with compliance matters related to U.S. federal and state privacy and data security laws, and more recently the GDPR and the California Consumer Privacy Act (CCPA), and the NYDFS Cyber Regulations.

With more than 30 years of consumer protection experience with the Federal Trade Commission (FTC),she provides clients with an in-depth perspective and working knowledge of the FTC its policy making efforts and enforcement activities. Specifically, she works with clients on Fair Credit Reporting Act (FCRA) and Gramm-Leach-Bliley Act (GLB Act) issues as well as the GDPR, CCPA and NY Cyber Regulations. Katherine also advises clients on advertising and marketing issues and other matters regulated by the FTC. Katherine is a United States Certified Information Privacy Professional (CIPP-US).

Katherine co-leads Drinker Biddle's Information Privacy, Security and Governance initiative, which brings together lawyers and professionals from across the firm to assist clients with assessing information privacy and security practices, developing information governance programs, responding to regulatory compliance inquiries and investigations, and handling litigation related to information privacy and security compliance. She also serves on the Editorial Board of the DBR on Data blog, which discusses developments in privacy, cybersecurity, information governance and data analytics.

While at the FTC, Katherine led numerous FCRA law enforcement investigations that resulted in consent decrees, and oversaw a number of FCRA rulemakings. She was also engaged in policy work in connection with data brokers and big data issues. Specifically, Katherine was part of the team that drafted the FTC's Data Broker Report and led the Big Data Workshop.

During her tenure at the FTC, Katherine also served as an attorney to former Chairman Janet Steiger and Commissioner Sheila Anthony. In those roles, she advised the Chairman/ Commissioner on the full range of consumer protection issues, including those involving privacy and unfair or deceptive acts or practices.

Katherine is a frequent speaker before industry conferences and other groups on privacy, data security, big data and FTC matters. She is co-chair of the American Bar Association's Privacy and Information Security Committee.

She is currently teaching a course at Marymount University's School of Business and Technology, titled "Law Policy and Ethics in the Information Age."

## Areas of Focus

### Services

- Intellectual Property
- Branding and Trademarks
- Due Diligence
- Intellectual Property Litigation
- Patents

### Industries

- InsurTech
- Enterprise Blockchains, Smart Contracts and Distributed Ledger Technology

DrinkerBiddle®

# Credentials

## Bar Admissions

- District of Columbia
- Virginia

## Education

- Lewis & Clark Law School, J.D.
- Pitzer College, B.A.

## Organizations

- Council of Better Business Bureaus, BBB EU Privacy Shield Dispute Resolution Procedure, Data Privacy Board (2017)
- American Bar Association, Section of Antitrust Law, Privacy and Information Security Committee, Co-Chair (2018-2021), Vice Chair (2016–2017)
- American Bar Association, Consumer Financial Services Committee, Federal and State Trade Practices Subcommittee, Chair (2015–2016); Vice-Chair (2011–2014)
- Episcopal Diocese of Virginia, Annual Council, Parish Delegate
- The Madeira School, McLean, VA, Board Member (2008–2016)

# Recognitions

- Official Commendation for Distinguished Service, Awarded by the Chairwoman of the Federal Trade Commission (2014)

DrinkerBiddle®


# Peter A. Blenkinsop

Partner | Washington, D.C.

peter.blenkinsop@dbr.com
Phone: (202) 230-5142


## About

**Peter A. Blenkinsop** advises clients on data privacy, research compliance, and e-health. He co-chairs the firm's Information Privacy, Security & Governance practice. Peter represents clients in the life sciences, health, nutrition, and technology sectors, among others.

Peter's focus on data privacy and security law began well over a decade ago in the run up to implementation of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Since then, his practice has expanded well beyond health information privacy to data privacy and security generally. He advises companies on compliance issues raised by US federal and state privacy laws such as the Children's Online Privacy Protection Act ("COPPA"), the CAN-SPAM Act, the Telephone Consumer Protection Act, and the Junk Fax Prevention Act. In this role, he assists clients in identifying privacy and security risks and developing information governance programs.

Peter also advises companies on compliance with international data transfer issues under the EU Data Protection Directive and other foreign privacy laws. He has assisted a number of multinationals in the development of their global privacy compliance programs. He regularly monitors and reports to clients on developments in data privacy laws worldwide.

As a member of the life sciences and pharmaceutical practices, Peter assists health industry clients with legal issues related to medical research, including clinical trials compliance, collection and use of human biological samples, and international research requirements. He advises companies on compliance with the Food and Drug Administration (FDA) and Department of Health and Human Services (HHS) human subject protection regulations, as well as guidelines for medical research issued by the International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use (ICH), World Health Organization, and World Medical Association.

Peter also advises companies on compliance with FDA and Federal Trade Commission (FTC) requirements related to the marketing of drugs, devices, and consumer healthcare products. This includes advising companies on development of mobile health applications, health websites, and health and fitness wearables.

## Areas of Focus

### Services

- Consortia Management
- Government and Regulatory Affairs
- Information Privacy, Security and Governance
- Clinical Research
- Information Privacy
- Information Security

### Industries

- Health Care
- Pharma and Life Sciences
- Enterprise Blockchains, Smart Contracts and Distributed Ledger Technology

## Credentials

### Bar Admissions

- District of Columbia
- Maryland

### Education

- Georgetown University Law Center, J.D., 2006, *magna cum laude*
- Yale University, B.A., 1999, *cum laude*

### Organizations

- District of Columbia Bar Association
- International Association of Privacy Professionals

DrinkerBiddle®


# Jeremiah Posedel

**Associate | Chicago**

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


## About

**Jeremiah Posedel** assists clients in two distinct but overlapping domains: (i) information technology transactions and (ii) information privacy and security. First, Jeremiah advises on and negotiates a wide array of transactions involving the acquisition, development and leveraging 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, HIPAA, COPPA, CAN-SPAM, TCPA, GLBA, PCI-DSS, DAA Program for Online Behavioral Advertising, and EU Data Protection Directive. 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, workplace monitoring, mobile device and app deployment, cross-border data transfers, clinical research and e-commerce initiatives.

Jeremiah is a Certified Information Privacy Professional (U.S./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
- Information Privacy, Security and Governance
- Cybersecurity and Incident Response Services

### 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*