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.

As Amended:
Changes to the CCPA for 2020 and Beyond

Presenters:
Peter Blenkinsop
peter.blenkinsop@dbr.com

Reed Abrahamson
reed.abrahamson@dbr.com

CCPA Webinar #6
September 16, 2019

Drinker Biddle

Webinar Schedule

1:00 – 2:00 PM US Eastern

- Today
- 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!

Next Webinar – Sept. 25

Preparing for CCPA Compliance: *Security, Incident Prevention, and Strategic Response*

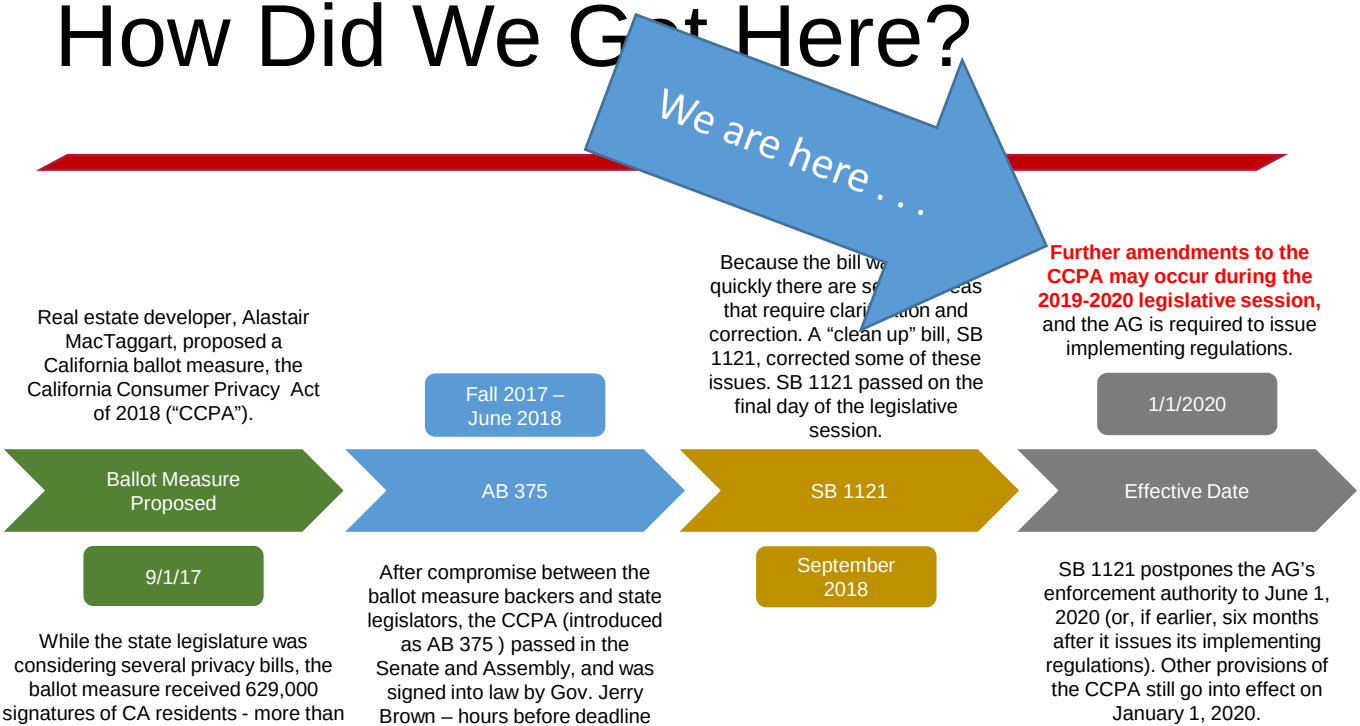
- **Pete Baldwin**, formerly of the National Security and Cybercrime Section of the U.S. Attorney's Office in the Eastern District of New York, and
- **Jason G. Weiss**, a former Supervisory Special Agent in the FBI Los Angeles Cyber and Forensics Branch

Agenda

- Brief Legislative History
- Overview of Key Amendments
- What to Expect Before 2020
- Questions

Brief Legislative History

How Did We Get Here?



Overview of Key Amendments

Note . . .

- Numerous “clean up” amendments made to update cross references, standardize language, and generally address issues of drafting.
  - E.g. “Web site” now “website” and “Internet” now “internet.”
- We’ll focus on the significant and substantive amendments.

CCPA 2020

Substantive Rights

1798.110(c)

(c) A business that collects personal information about consumers shall disclose, pursuant to subparagraph (B) of paragraph (5) of subdivision (a) of Section 1798.130:

(1) The categories of personal information it has collected about ~~that~~ consumer[s].

(2) The categories of sources from which the personal information is collected.

(3) The business or commercial purpose for collecting or selling personal information.

(4) The categories of third parties with whom the business shares personal information.

(5) ~~The~~[That a consumer has the right to request the] specific pieces of personal information the business has collected about that consumer.

CCPA 2020

Implications

- Right to information no longer customized to the consumer visiting the website:
  - Generic to “consumers” generally
  - Disclosure of *further* right to request specific pieces of information, but not required in website policy itself.
- Note – equivalent changes *not* made to text of 1798.110(a)

1798.115(a)

(a) A consumer shall have the right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer:

(1) The categories of personal information that the business collected about the consumer.

(2) 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.

CCPA 2020

Implications

- Disclosure of third parties to whom information is sold no longer requires identifying *each* third party
- CCPA does not define “categories” of third parties, unlike the definition of “categories” of personal information.

1798.125(a)

(a) (1) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by:

(A) Denying goods or services to the consumer.

(B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

(C) Providing a different level or quality of goods or services to the consumer.

(D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

(2) 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.

CCPA 2020

Implications

- Removes difficult-to-apply requirement that incentives be related to the value of consumer data *to the consumer* and replaces with reference to the value to the *business*
- Allows companies to determine whether consumer opt-outs affect the price charged by consumer.
- Same change made to 1798.125(b).
- References in 1798.125 to notice requirements adjusted to refer to 1798.130 (which does address notice) and not 1798.135 (which did not address notice).

1798.130(a)

(a) In order to comply with Sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125, a business shall, in a form that is reasonably accessible to consumers:

(1) (A) Make available to consumers two or more designated methods 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.~~ A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information 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.

Implications

- Not as helpful to most businesses as earlier drafts, and likely requires the maintenance of a toll-free number for businesses with “brick and mortar” facilities.

Personal Information

1798.140(o)(1)

(o) (1) "Personal information" means 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:

CCPA 2020

Implications

- Appears to provide carve out for information not reasonably capable of being associated with a person.
- However, “reasonably” does not modify “identifies,” “relates to” or “describes.”

1798.140(o)(2), (3)

(2) "Personal information" does not include publicly available information. For ~~these~~ purposes of this paragraph, "publicly available" means information that is lawfully made available from federal, state, or local government records~~, if any conditions associated with such information~~. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge.

(3) "Personal Information ~~is not "publicly available" if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained. "Publicly available~~" does not include consumer information that is deidentified or aggregate consumer information.

CCPA 2020

Implications

- Removes difficult to apply standard for “publicly available” which required interpretation of the “purpose” for which records were released by the government.
- “Publicly available” still limited to government records.

New Exemptions

Exemptions for . . .

- "Do Not Sell" Requirement as applied to vehicle ownership information shared between dealers and manufacturers for repairs covered by warranty or recalls.
- Broader exception for consumer reports subject to FCRA
- Until 2021 – information about employees, officers, job applicants and contractors, including information about those person's emergency contacts or benefits beneficiaries.
  - Notice still required, and these individuals may still bring suit for a data breach.

Exemptions for . . .

(1) The obligations imposed on businesses by Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, and 1798.135 shall not apply to personal information reflecting a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who is acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit, or government agency and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, nonprofit or government agency.

CCPA 2020

Implications

- Business-to-business data still subject to “do-not-sell” requirements.

1798.145(k)

(~~j~~k) This title shall not be construed to require a business to collect personal information that it would not otherwise collect in the ordinary course of its business, retain personal information for longer than it would otherwise retain such information in the ordinary course of its business, or reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

CCPA 2020

Implications

- Exemption more aligned with exemptions in GDPR
- Clarifies that business are not required to collect additional information to verify consumer requests or otherwise implement consumer rights

Private Right of Action

1798.150(a)

(a) (1) Any consumer whose nonencrypted ~~or~~and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

(A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

CCPA 2020

Implications

- Narrows scope of private right of action by requiring that information be *both* not encrypted and not redacted before it triggers right to sue.

What to Expect Before 2020

Still to come . . .

- Governor Signature
- Draft AG Regulations
  - Originally anticipated this fall
  - Likely will include discussion of “verifiable consumer request”

Questions?

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*

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

Industries

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

Credentials

Bar Admissions

- Illinois

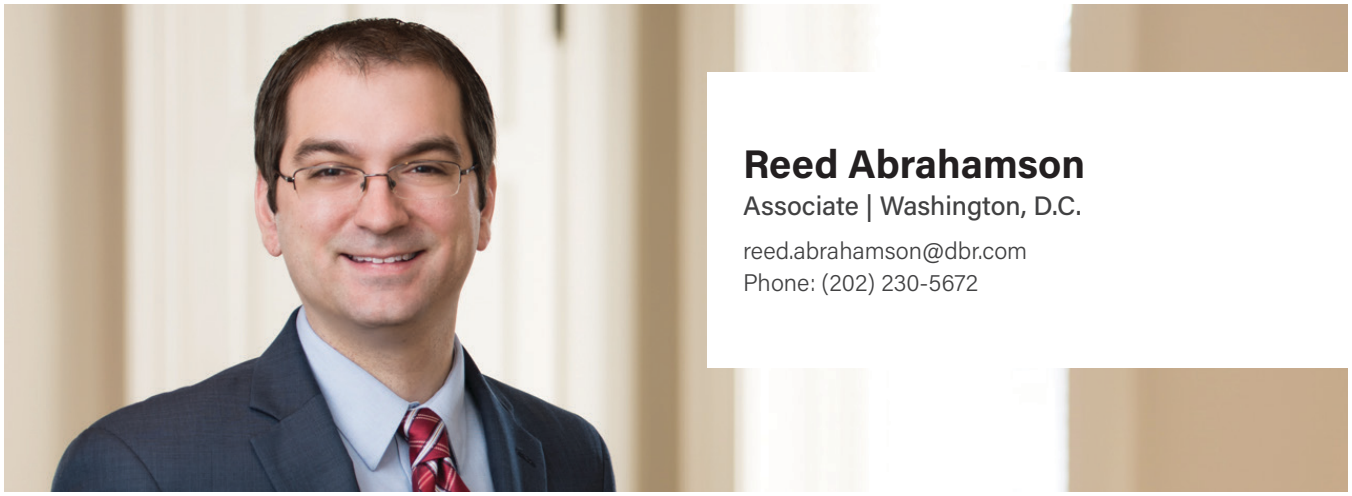
Court Admissions

- 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