WILMERHALE®

WILMER CUTLER PICKERING HALE AND DORR LLP®

Legislative and Regulatory Updates on the CCPA and Similar Bills in Other States

October 8, 2019

Reed Freeman

reed.freeman@wilmerhale.com

Attorney Advertising

Webinar Guidelines

- Participants are in listen-only mode
- Submit questions via the Q&A feature
- Questions will be answered as time permits
- Offering 1 CLE credit in California and New York*

WilmerHale has been accredited by the New York State and California State Continuing Legal Education Boards as a provider of continuing legal education. This program is being planned with the intention to offer CLE credit in California and non-transitional CLE credit in New York. This program, therefore, is being planned with the intention to offer CLE credit for experienced New York attorneys only. Attendees of this program may be able to claim England & Wales CPD for this program. WilmerHale is not an accredited provider of Virginia CLE, but we will apply for Virginia CLE credit if requested. The type and amount of credit awarded will be determined solely by the Virginia CLE Board. Attendees requesting CLE credit must attend the entire live program. CLE credit is not available for those who watch on-demand webinar recordings.

The California Consumer Privacy Act (CCPA) – Brief Overview

Definitions – “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:”

- Annual gross revenues above **$25 mm**;
- Annually buys, receives, sells, or shares personal information of **50,000 or more consumers** (California residents); or
- Derives **50 percent or more of its annual revenues** from selling consumers’ personal information.

(1798.140(c))

Legislative note: “Consumer” is currently defined as any California resident. AB 25 and AB 1355, pending signature from the governor after passing the legislature, will create a one-year exemption for employees and other individuals whose data is collected in the context of their job (*i.e.*, “business-to-business data”).

Definitions – "Personal information"

"**Personal information**" means 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.* (1798.140(o)(1))

Includes, but is not limited to, the following, if they meet the test above:

(A) Identifiers such as a real name, alias, postal address, *unique personal identifier, online identifier, Internet Protocol address, email address,* account name, social security number, driver's license number, passport number, or other similar identifiers.

(D) Commercial information, including records of personal property, *products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies*.

(F) *Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement*.

(G) *Geolocation data*.

(K) *Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes*.

Legislative note: AB 874, pending signature from the governor after passing the legislature, will add "reasonably" before "capable of being associated with."

Definitions – “Deidentified” and “aggregate” data

“Deidentified” and “Aggregate consumer information” are not expressly excluded from the definition of “personal information” (potentially due to drafting errors).

— However, the CCPA’s obligations *“shall not restrict a business’s ability to . . . collect, use, retain, sell, or disclose consumer information that is deidentified or aggregate consumer information.”* (1798.145(a)(5))

Definitions – “Deidentified” and “aggregate” data

<u>But note the definitions of “Deidentified” and “Aggregate Consumer Information”: Do you meet them?</u>

“<u>Deidentified</u>” means information that *cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer,* provided that a business that uses deidentified information:

(1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.

(2) Has implemented business processes that specifically prohibit reidentification of the information.

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

(4) Makes no attempt to reidentify the information. (<u>1798.140(a)</u>)

“<u>Aggregate consumer information</u>” means 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.* (<u>1798.140(h)</u>)

<u>Practice tip</u>: If you refer to personal information you hold as “deidentified” or “aggregate,” you must meet these definitions or risk a cause of action for deceptive or unfair trade practices.

Definitions – "Sell"

"Sell" – It's not your mother's definition.

"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.* (1798.140(t)(1))

Awaiting clarification from the AG in guidance or discretionary rulemaking. But for now, means providing to another entity that is not a "service provider" in a commercial context.

VERY BROAD.

Definitions – "Sell" exemptions

The CCPA contains various exemptions to the definition of "sell," including:

- Sharing based on consumer consent: 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 this title.* (1798.140(t)(2)(A))
- Sharing for opt-outs. (1798.140(t)(2)(B))
- Sharing with service providers: The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose if (i) the business has provided notice that information being used or shared in its terms and conditions; and (ii) the *service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.* (1798.140(t)(2)(C))

Application:

- **Record consent to sharing.**
- **DPA-style contracts with service providers required.**

Definitions – "Service provider"

"Service provider" is defined as: 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 this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business." (1798.140(v))

Application: Contracts with service providers required.

California Service Provider Addendum

What is required?

- Ensure the service provider meets the CCPA's definition.
- Will process only on behalf of business—no other retention, use, disclosure.
- Will not "sell."

Combine with GDPR DPA?

- Pros: Simplicity & consistency.
- Cons: Definitions are inconsistent; must apply broadest restrictions to everyone (*i.e.*, GDPR rights apply to CCPA "personal information").
- **We recommend having a separate CCPA addendum—can be one page.**

Obligations – Disclosure of personal information collected

<u>“Businesses” that sell personal information or that disclose it for a business purpose must, in response to a verified request from a consumer, disclose:</u>

- Categories of personal information that the business collected about the consumer;
- 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 to whom the personal information was sold;* or if the business has not sold consumers’ personal information, it shall disclose that fact; and
- Categories of personal information that the business disclosed about the consumer for a business purpose; or if the business has not disclosed the consumers’ personal information for a business purpose, it shall disclose that fact.

(<u>1798.115</u>, <u>1798.130(a)(4), (a)(5)(C)</u>)

<u>Application</u>: Data mapping against the extremely broad definition of “personal information” is very difficult!

Obligations – Deletion of personal information

“Businesses” must, in response to a verifiable consumer request, delete personal information of the requester and make sure service providers do as well, with certain exceptions. (1798.105(a),(c)-(d))

- The California AG must adopt regulations to clarify what is a “verifiable consumer request.”
- The CCPA states it *“shall not be construed to require a business to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.”* (1798.145(i)) (But see extremely broad definition of personal information).

Application: Compliance depends on data mapping. Deleting all “personal information” is also extremely difficult!

Obligations – Opt-out for sales of personal information

“Businesses” may not sell personal information without giving notice and a chance for affected consumers to opt out.

- “Businesses” must place a **link on their website homepage titled “Do Not Sell My Personal Information”** that redirects to a webpage that enables a consumer to opt-out of the sale of the consumer’s personal information.
- “Homepage” is defined to include any page where personal information is collected.
- The business cannot require consumers to create an account in order to opt-out of the sale of their personal information.
- (1798.120, 1798.115(d), 1798.135)

Application: Opt-out link must be provided if business “sells” personal information to anyone other than “service providers,” as defined.

Obligations – Enhanced disclosures of privacy rights and practices

“Businesses” must disclose in their online privacy policy or California-specific description of consumer privacy rights consumers’ rights under the CCPA and the methods for exercising those rights, as well as the categories of personal information the business collects, sells, or discloses for business purposes. (1798.130(a)(5))

- The notices must be updated annually.

Application:

- **PP must be updated by 1/1/20.**
- **Moving target.**
- **Then update annually.**

CCPA Enforcement

Enforcement

AG – Whole law and regs

- Injunction and civil penalties of not more than $2,500 for each violation or $7,500 for each intentional violation.
- **Draft regs expected any day**; then comments; final regs could come in March or April 2020.
- Enforcement begins six months after final regs or July 1, 2020 (whichever is sooner).
- Notably, the AG does not like the law and has said his office will not initially bring a host of cases.

PRA – Breach

- Not less than $100 and not greater than $750 per consumer per incident; or actual damages, whichever is greater.
- Injunctive or declaratory relief.
- Any other relief the court deems proper.
- No six month grace period before enforcement.
- Average TCPA settlement: Roughly $5-6 million (plus costs of defense).

CCPA Amendments

Successful amendments (pending signature from governor)

- AB 25 – Employee exemption.
  - One-year sunset – Negotiations with Labor expected.
  - No exemption from requirement to notify of categories collected and purpose.
- AB 1355 – Various changes, including “business-to-business” exemption.
  - One-year sunset – Negotiations with Labor expected.
  - No exemption from opt-out of sale or non-discrimination provision.
- AB 874 – Removes limitations on use of publicly available information; adds “reasonably” before “capable of being associated with.”
- AB 1564 – Allows online-only businesses to provide a physical address for consumer requests instead of a toll-free telephone number.

Failed amendments

- SB 753 – Would have exempted online advertising from definition of “sale.”
- AB 846 – Would have clarified that loyalty and rewards programs do not violate nondiscrimination section.
  - Industry expected to pursue next session.
- AB 873 – Some changes moved to other bills; would also have modified definition of “deidentified.”

Other State Legislation

State Legislation – General Trends

- **Nevada** passed a limited "do not sell" bill.
- Larger CCPA "copycat" bills were introduced in at least 14 states, but none have passed.
  - Notable examples include **New Jersey** and **Massachusetts** (which could still pass this year) and **Washington** (expected to pass in some form next year).
- Common modifications to the CCPA in copycat bills include:
  - Expanding the private right of action (MA, NY).
  - Modifying the thresholds for covered businesses (MA, NY, PA, RI).
  - Removing the requirement to disclose "specific pieces" of information collected (NY, TX).
  - Removing various exemptions for data subject to other laws (NY, RI).

State Legislation – General Trends

- Other bills reflect privacy concerns regarding:
  - Internet service providers (*e.g.*, ME (passed) MT, NY).
  - Data brokers (*e.g.*, CA).
  - Social media companies (*e.g.*, CA, LA).
  - Minors' personal information (*e.g.*, CT, VA).
  - Geolocation information (*e.g.*, IL).

Nevada – S.B. 220

- Took effect October 1.
- Creates a "Do Not Sell" right.
- Fixes many problems with broad and confusing CCPA definitions—compliance is easier.
  - Applies to "covered information" collected online: First/last name, address, email, phone #, SSN, other **PII.**
  - **"Sell" means sell to a data broker.**
- Must opt-out from sale upon verifiable request within 60 days.
- No private right of action.

New Jersey – A.B. 4902 / S.B. 2834

- Significantly different language from CCPA (less confusing, but still very broad).
- "Personally identifiable information" defined similarly to CCPA's "personal information"—information "able to be associated with" a customer.
- Requires disclosure of **specific third parties** that receive PII.
- Access right only applies to information disclosed to third parties.
- "Do Not Sell" right (really means "do not disclose").
- No verification of consumer requests.
- No right to delete.

Massachusetts – S.B. 120

- Hearing yesterday.
- CCPA copycat—rights to notice of “personal information” collected; deletion; and opt-out from sale.
- Adds right to request names of third parties receiving PI.
- Includes employee exemption.
- Revenue threshold for covered businesses lowered to $10 million (from $25 million in the CCPA); no threshold for number of consumers.
- Private right of action: Damages of $750 per person per incident, or actual damages.

Washington – *Washington Privacy Act (S.B. 5376/H.B. 1854)*

- Passed Senate, but House failed to pass before the legislative session ended.
- Expected to be reintroduced in the next session.
- Applies to “legal entities” (1) that either control or process data of at least 100,000 Washington consumers or (2) that derive more than 50% of their gross revenue from the sale of personal information and process or control data of at least 25,000 Washington consumers.
- Like the GDPR, distinguishes between *“controllers,”* which “determine the purposes and means of the processing of personal data,” and *“processors,”* which “process data on behalf of the controller.”
- Controllers are “responsible for meeting the obligations under this act;” processors “are responsible . . . for adhering to the instructions of the controller and assisting the controller to meet its obligations.”

Washington – Washington Privacy Act (S.B. 5376/H.B. 1854)

- **On request, controllers would be required to:**
  - "*Provide a copy* of the personal data undergoing processing" in a *portable format*;
  - "*Correct* inaccurate personal data concerning the consumer" without undue delay;
  - "*Delete* the consumer's personal data without undue delay" in a number of circumstances and "take reasonable steps, which may include technical measures, to inform other controllers that are processing the personal data that the consumer has requested the deletion by the other controllers of any links to, or copy or replication of, the personal data;" and
  - "*Restrict processing*" of the consumer's personal data in various circumstances.
- In the Senate bill, these requirements only apply to personal data "that the controller maintains in identifiable form." The requirement to notify other controllers is also limited to controllers "of which [the business] is aware."

Washington – Washington Privacy Act (S.B. 5376/H.B. 1854)

- Controllers must publish privacy notices that are “reasonably accessible to consumers” in a “clear, meaningful” form that “includes: (a) The *categories of personal data collected* by the controller; (b) The purposes for which the categories of personal data are used and disclosed to third parties, if any; (c) The rights that consumers may exercise pursuant to section 6 of this act, if any; (d) The *categories of personal data that the controller shares with third parties, if any;* and (e) The *categories of third parties,* if any, with whom the controller shares personal data.”
- Controllers that sell personal data to data brokers or use personal data for direct marketing must disclose such processing and provide an opportunity for consumers to object.
  - In the House version of the bill, controllers that engage in profiling must also disclose that, including the logic used.

Washington – Washington Privacy Act (S.B. 5376/H.B. 1854)

- Controllers “must conduct and document risk assessments” regularly.
- “A controller or processor that uses *deidentified data* must exercise *reasonable oversight to monitor compliance with any contractual commitments* to which the deidentified data is subject, and must take appropriate steps to address any breaches of contractual commitments.”

Where are we with federal legislation?

Federal privacy legislation

- Working group in Senate Commerce Committee.
- Spearheaded by Senators Blumenthal and Moran.
- House version in progress as well.
- Draft bills expected, but **very** unlikely to pass this session.
- Don't expect progress **unless and until** several states pass inconsistent laws.
- Major issues:
  - **Business must have preemption—and advocates know it.**
  - Additional authority for FTC likely (rulemaking and/or civil penalty).

Questions?

Contact

D. Reed Freeman, CIPP/US
Co-Chair, Big Data Practice

Co-Chair, Cybersecurity and Privacy Practice

- reed.freeman@wilmerhale.com
- (202) 663-6267

Wilmer Cutler Pickering Hale and Dorr LLP is a Delaware limited liability partnership. WilmerHale principal law offices: 60 State Street, Boston, Massachusetts 02109, +1 617 526 6000; 1875 Pennsylvania Avenue, NW, Washington, DC 20006, +1 202 663 6000. Our United Kingdom office is operated under a separate Delaware limited liability partnership of solicitors and registered foreign lawyers authorized and regulated by the Solicitors Regulation Authority (SRA No. 287488). Our professional rules can be found at www.sra.org.uk/solicitors/code-of-conduct.page. A list of partners and their professional qualifications is available for inspection at our UK office. In Beijing, we are registered to operate as a Foreign Law Firm Representative Office. This material is for general informational purposes only and does not represent our advice as to any particular set of facts; nor does it represent any undertaking to keep recipients advised of all legal developments. Prior results do not guarantee a similar outcome.