WILMERHALE

WILMER CUTLER PICKERING HALE AND DORR LLP ®

Privileged and Confidential

Privacy: California and the Growing Storm

April 10, 2019

Jonathan G. Cedarbaum

bpi BITS

Roadmap

I. California Consumer Privacy Act (CCPA)

II. State Legislative Activity

III. Federal Legislative Activity

CCPA: Basics

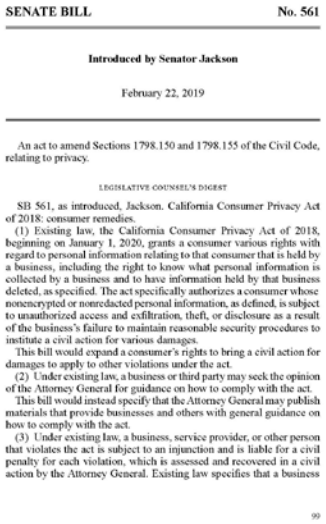
- Enacted June 2018; amended September 2018
- Effective January 1, 2020; regulations due by July 1, 2020; no AG enforcement until 6 months after required regulations published or July 1, 2020
- Key Requirements:
  - Notice at point of collection about categories of personal information collected and purposes for which used
  - Upon verified request, disclosure of categories and specific personal information collected, sold, or disclosed for a commercial purpose; categories of sources; categories of third parties with whom shared
  - Upon verified request, deletion of personal information collected and direction to service providers to do so
  - Opt-out from sales of personal information; opt-in for those less than 16 years old
  - Notice of CCPA rights

CCPA: Legislative Activity

- Many proposed bills, both supported by the business community and by consumer privacy organizations
  - 16 CCPA
  - 3 data breach
  - 2 data valuation
- Substantial amendments unlikely
- Most plausible favorable amendment: clarification that employees are not included in definition of “
- If amendments enacted, likely to expand the law’s requirements further

CCPA: Legislative Activity: SB 561 (Jackson)

- Private right of action for violation of any rights under the CCPA, not just data breaches
- Elimination of 30-day right to cure
- Elimination of AG advisory opinion obligation
- Hearing yesterday



SENATE BILL No. 561

Introduced by Senator Jackson

February 22, 2019

An act to amend Sections 1798.150 and 1798.155 of the Civil Code, relating to privacy.

LEGISLATIVE COUNSEL'S DIGEST

SB 561, as introduced, Jackson. California Consumer Privacy Act of 2018: consumer remedies.

(1) Existing law, the California Consumer Privacy Act of 2018, beginning on January 1, 2020, grants a consumer various rights with regard to personal information relating to that consumer that is held by a business, including the right to know what personal information is collected by a business and to have information held by that business deleted, as specified. The act specifically authorizes a consumer whose nonencrypted or nonredacted personal information, as defined, is subject to unauthorized access and exfiltration, theft, or disclosure as a result of the business's failure to maintain reasonable security procedures to institute a civil action for various damages.

This bill would expand a consumer's rights to bring a civil action for damages to apply to other violations under the act.

(2) Under existing law, a business or third party may seek the opinion of the Attorney General for guidance on how to comply with the act.

This bill would instead specify that the Attorney General may publish materials that provide businesses and others with general guidance on how to comply with the act.

(3) Under existing law, a business, service provider, or other person that violates the act is subject to an injunction and is liable for a civil penalty for each violation, which is assessed and recovered in a civil action by the Attorney General. Existing law specifies that a business

99

CCPA: Rulemaking

- Rulemaking process: seven public forums; 1300+ pages of public comments; draft regulations expected in the fall; final regulations due by January 1, 2020
- Seven mandatory subjects for rulemaking:

  (1) categories of personal information

  (2) definition of unique identifiers

  (3) exceptions to CCPA for compliance with other laws, e.g., trade secrets, other IP rights

  (4) submitting and complying with requests

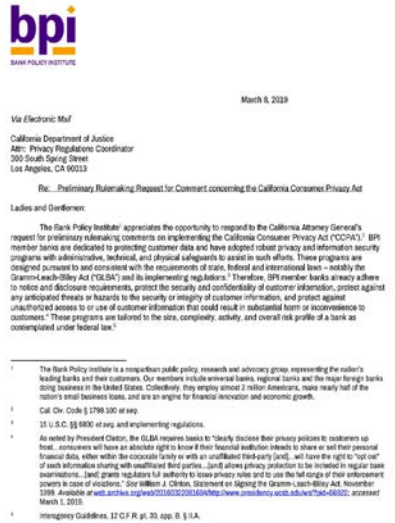
  (5) uniform opt-out logo/button

  (6) notices and information to consumers, including financial incentive offerings

  (7) verification of consumer requests

CCPA: Selected Rulemaking or Compliance Issues

- Definition of “personal information”: linkable to household as well as person
- Definition of “consumer”: employees, contractors, job applicants
- “Look back” period trigger date
- How to verify consumer requests



bpi
BANK POLICY INSTITUTE

March 8, 2019

Via Electronic Mail

California Department of Justice
Attn: Privacy Regulations Coordinator
300 South Spring Street
Los Angeles, CA 90013

Re: Preliminary Rulemaking Request for Comment concerning the California Consumer Privacy Act

Ladies and Gentlemen:

The Bank Policy Institute[1] appreciates the opportunity to respond to the California Attorney General's request for preliminary rulemaking comments on implementing the California Consumer Privacy Act ("CCPA").[2] BPI member banks are dedicated to protecting customer data and have adopted robust privacy and information security programs with administrative, technical, and physical safeguards to assist in such efforts. These programs are designed pursuant to and consistent with the requirements of state, federal and international laws – notably the Gramm-Leach-Bliley Act ("GLBA") and its implementing regulations.[3] Therefore, BPI member banks already adhere to notice and disclosure requirements, protect the security and confidentiality of customer information, protect against any anticipated threats or hazards to the security or integrity of customer information, and protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to customers.[4] These programs are tailored to the size, complexity, activity, and overall risk profile of a bank as contemplated under federal law.[5]

---

1 The Bank Policy Institute is a nonpartisan public policy, research and advocacy group, representing the nation's leading banks and their customers. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ almost 2 million Americans, make nearly half of the nation's small business loans, and are an engine for financial innovation and economic growth.

2 Cal. Civ. Code § 1798.100 *et seq.*

3 15 U.S.C. §§ 6800 *et seq.* and implementing regulations.

4 As noted by President Clinton, the GLBA requires banks to "clearly disclose their privacy policies to customers up front…consumers will have an absolute right to know if their financial institution intends to share or sell their personal financial data, either within the corporate family or with an unaffiliated third-party [and]…will have the right to "opt out" of such information sharing with unaffiliated third parties…[and] allows privacy protection to be included in regular bank examinations…[and] grants regulators full authority to issue privacy rules and to use the full range of their enforcement powers in case of violations." *See* William J. Clinton, Statement on Signing the Gramm-Leach-Bliley Act. November 1999. *Available at* web.archive.org/web/20160320016044/http://www.presidency.ucsb.edu/ws/?pid=58022; accessed March 1, 2019.

5 Interagency Guidelines. 12 C.F.R. pt. 30. app. B. § II.A.

How does the CCPA compare to the GDPR?

Topic	GDPR	CCPA
Scope	Article 3: Applies to a "controller" or "processor": • Established in the EU, or • Established outside of the EU and offering goods/services or monitoring behavior in the EU.	A for-profit "business" that does business in CA and meets revenue or volume threshold. "Business" is defined more broadly than an EU "controller"; includes any entity that receives personal information.
Definition of personal data/information	Article 4: Any data relating to an identified or identifiable natural person	Data "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" Extremely broad definition
Lawful processing requirements	Article 6: Must have a valid legal basis for all processing of personal data	No legal basis required, but must provide substantive rights
Notice requirements	Article 13: Must provide data subjects with detailed notice about the collection, use, and disclosure of personal data, as well as retention period, individual rights, bases for processing, identity of controller/DPO/representative	Must disclose certain information about the collection, sale, and disclosure of personal information in privacy policy or on website Must provide disclosures at or before the collection of personal information "Do Not Sell My Personal Information" link

How does the CCPA compare to the GDPR?

Topic	GDPR	CCPA
Right to access	Article 15: Must provide data subjects with "access to [their] personal data," as well as specific details about processing Exceptions: (a) can verify identity, (b) manifestly unfounded or excessive requests, (c) adversely affects the rights and freedoms of others	Must provide consumers with details about collection, sale, and disclosure of their personal information as well as "specific pieces of personal information" Exceptions: (a) can verify identity, (b) manifestly unfounded or excessive requests
Right to delete	Article 17: Data subjects have a right to have their personal data deleted where (a) "no longer necessary," (b) they withdraw consent, (c) processing is unlawful, or (d) if processing is based on legitimate interests, there are no "overriding legitimate grounds" Exceptions: (i) continued lawful basis for processing, (ii) exercising right of expression, (iii) compliance with EU law, (iv) establishment / exercise / defense of legal claims, (v) public health exception, (vi) archiving / research exception	Consumers have a generally applicable right to have their personal information deleted Exceptions: (i) complete a transaction / perform a contract, (ii) detect / protect against / prosecute security incidents or illegal activity, (iii) debug and fix errors, (iv) exercise free speech or other legal rights, (v) research, (vi) "solely internal uses that are reasonably aligned" with consumer expectations, (vii) compliance with law, (viii) other uses that are "compatible with the context in which the consumer provided the information"
Right to object	Article 21: Data subjects have a right to object to the processing of their personal data in certain circumstances	Consumers have a right to opt out of the "sale" of their personal information

How does the CCPA compare to the GDPR?

Topic	GDPR	CCPA
Right to data portability	Article 20: Data must be provided "in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance"	Data must be provided "in a portable and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit the information to another entity without hindrance"
Time for responding to consumer requests	Article 12: "Without undue delay" and in any event within one month Can be extended by two months "where necessary"	Within 45 days of receiving a verifiable request Can be extended by 45 days "when reasonably necessary"
Cross-border transfer requirements	Article 46: Transfers of personal data outside of the EU must comply with safeguard requirements (e.g., adequacy, contractual clauses)	None
Fines	Article 83: Infringements may result in administrative fines up to €20 million or 4% of total worldwide annual turnover, whichever is greater Private right of action for actual damages	The Attorney General may impose civil penalties of up to $2,500 per violation or $7,500 per intentional violation. There is no cap on the total amount of the penalty Private right of action for data breaches ($100-$750 or actual damages) But 30-day cure period for AG or private actions

State Legislative Activity: Overview

- CCPA, tech company data handling controversies have prompted pervasive focus on increasing privacy protections in state laws; also encouraged by widespread perception that Congress is largely incapable of significant legislative achievements

- 14 major bills reviewed in Feb. 20 handout; many more since then; many more targeted ones

- Washington State:
  - one of most comprehensive, likely to be enacted:
  - passed state senate by overwhelming majority March 6; hearing before House Economic Development Committee March 22;
  - governor has said he will sign it

State Bills Modeled on the CCPA

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

Current status: The Senate version was introduced in January 2019 and referred to the Committee on Environment, Energy and Technology, which held a hearing on January 22. A substitute Senate version was introduced in February 2019 and referred to the Ways and Means Committee. The House version was introduced in February 2019 and referred to the Technology and Economic Development Committee, which held a hearing on February 12.

Key provisions:

- The bill would apply only to "legal entities" that either control or process data of at least 100,000 Washington consumers or 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 CCPA, there are exemptions in the bill for data covered by other federal or state privacy laws, such as HIPAA and GLBA.
- Like the GDPR, the bill 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."

State Bills Modeled on the CCPA

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

Key provisions (Continued):

- **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."
- The Senate version of the bill would require controllers to respond to consumer requests within 30 days of receipt, which could be extended by 60 additional days where reasonably necessary.

State Bills Modeled on the CCPA

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

Key provisions (continued):

- 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 is 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.
- 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."
- The Attorney General would be authorized to enforce the law, and violations would be defined as unfair trade practices. The bill would establish an "office of privacy and data protection" in the office of the state chief information officer "to serve as a central point of contact for state agencies on policy matters involving data privacy and data protection."

State Bills Modeled on the CCPA

Hawaii – S.B. 418

- Current status:
  - The bill was introduced in January 2019 and referred to the Commerce, Consumer Protection, and Health Committee.
- Key provisions:
  - Modeled closely on the CCPA, the bill would give consumers rights to notice of "identifying information" collected and parties with whom such information is shared; deletion; and opt-out from sale.
  - The definition of "consumer" is broader than in the CCPA; it includes any individual "who interacts with a business" in Hawaii (instead of residents of the state).
  - Covered businesses would not be limited by any revenue or affected consumer thresholds.
  - The CCPA's exemptions for data covered by various federal laws are omitted.
  - No data breach provisions are included.

State Bills Modeled on the CCPA

Maryland – Online Consumer Protection Act (S.B. 613/H.B. 901)

Current status: The Senate version was introduced in February 2019 and referred to the Finance Committee. The committee is scheduled to hold a hearing on March 8. The House version was introduced in February 2019 and referred to the Economic Matters Committee. The committee is scheduled to hold a hearing on March 6.

Key provisions:

- Modeled closely on the CCPA, the bill would give consumers rights to notice of "personal information" collected and parties with whom such information is shared; deletion; and opt-out from third-party disclosures.
- In the definition of covered businesses, the affected consumer threshold is 100,000 users (rather than the 50,000 in the CCPA).
- In definition of "personal information," the CCPA's list of examples has been omitted, though the definition remains similar in scope. Unlike in the CCPA, personal information must relate to an individual or their device, not a household.
- The bill changes the CCPA's restrictions on "sales" to apply to "third-party disclosures."

State Bills Modeled on the CCPA

Massachusetts – S.B. 120

Current status: The bill was introduced in January 2019 and referred to the Joint Committee on Consumer Protection and Professional Licensure.

Key provisions:

- Modeled closely on the CCPA, the bill would give consumers rights to notice of "personal information" collected and parties with whom such information is shared; deletion; and opt-out from sale.
- The bill includes an exemption for collection and disclosure of employee personal data within the scope of its role as employer that does not appear in the CCPA.
- The annual gross revenue threshold for covered businesses is $10 million (rather than $25 million in the CCPA) and the provision including companies with more than 50,000 users is omitted.
- The bill would create a private right of action for any violation, with damages of $750 per person per incident, or actual damages.
- Massachusetts AG could seek penalties of up to $2,500 per violation and $7,500 per intentional violation.

State Bills Modeled on the CCPA

New Mexico – Consumer Information Privacy Act (S.B. 176)

Current status: The bill was introduced in January 2019 and referred to the Corporations & Transportation Committee.

Key provisions:

- Modeled closely on the CCPA, the bill would give consumers rights to notice of "personal information" collected and parties with whom such information is shared; deletion; and opt-out from sale.
- The definition of "personal information" is limited to information from federal, state, or local government records.
- The bill would not apply to information collected or used pursuant to other state or federal laws if the application is in conflict with that law, as clarified in regulations issued by the Attorney General.

State Bills Modeled on the CCPA

Rhode Island – Consumer Privacy Protection Act (S.B. 234)

Current status: The bill was introduced in January 2019 and referred to the Judiciary Committee.

Key provisions:

- Modeled closely on the CCPA, the bill would give consumers rights to notice of "personal information" collected and parties with whom such information is shared; deletion; and opt-out from sale.
- The annual gross revenue threshold for covered businesses is $5 million.
- The bill contains no exemptions for personal information collected or used pursuant to other laws.
- The bill contains no provisions granting rulemaking and enforcement authority to the Attorney General.

Federal Legislative Activity: Overview

- Four major hearings so far, focused on principles rather than bills:
  - House Energy and Commerce: Feb. 26
  - Senate Commerce: Feb. 27
  - Senate Judiciary: March 12
  - Senate Commerce Consumer Protection Subcommittee: March 26
- Bipartisan working groups on House and Senate Commerce Committees
- Some key points of debate:
  - Federal preemption
  - Use limitations and individual rights
  - Small business or startup carve-outs
  - FTC authority
  - Private right of action

Federal Bills

American Data Dissemination (ADD) Act (S. 142)

Current status: Introduced by Sen. Rubio (R-FL) in January 2019, the bill has been referred to the Committee on Commerce, Science, and Transportation.

Key provisions:

Would not impose substantive requirements, but would create a process for establishing requirements for companies that "provide services using the Internet" akin to the requirements that apply to federal agencies under the Privacy Act.

The FTC would have six months from the ADD Act's enactment to submit recommendations to Congress for privacy legislation that would be "substantially similar, to the extent practicable, to the requirements applicable to agencies under the Privacy Act of 1974."

If Congress fails to enact a qualifying law within two years of the ADD Act's enactment, the FTC would be required to promulgate final regulations in the following three months based on the ADD Act's specifications.

Federal Bills

American Data Dissemination (ADD) Act (S. 142) (continued)

Those specifications include:

- A prohibition on disclosure without prior consent except under specific exemptions, including when the use is compatible with the purpose of collection;
- An obligation to keep records of disclosures;
- access and correction rights;
- An exemption for certain small, newly formed businesses;
  - Exemptions for personal information governed by the Health Insurance Portability and Accountability Act (HIPAA) and its regulations or by the Family Educational Rights and Privacy Act of 1974 (FERPA);
  - FTC authority to resolve possible conflicts between ADD Act and the Children's Online Privacy Protection Act (COPPA) or Gramm-Leach Bliley Act (GLBA) and their implementing regulations; and
  - Enforcement by the FTC.

Preemption: ADD Act or regulations would supersede state law "relating to a covered provider, to the extent that the provision relates to the maintenance of: (1) records covered by [the ADD] Act; or (2) any other personally identifiable information or personal identification information."

Federal Bills

Social Media Privacy and Consumer Rights Act (S. 189)

Current status: Originally introduced by Sen. Klobuchar (D-MN) and Sen. Kennedy (R-LA) in April 2018 (as S. 2728), the bill was reintroduced in January 2019 and referred to the Committee on Commerce, Science, and Transportation.

Key provisions:

- Operators of "covered online platforms," defined as "any public-facing website, web application, or digital application (including a mobile application)," would be required:

– to give consumers prior notice and the ability to opt out of collection and use by third parties of "personal data of the user produced during the online behavior of the user, whether on the online platform or otherwise," both when the user first opens an account and whenever a new product results in new forms of data collection or use;

-- to disclose terms of service, including concerning collection and use of personal data, in a form that is "easily accessible," "of reasonable length," "clearly distinguishable from other matters," and stated in "language that is clear, concise, and well organized";

-

Federal Bills

Social Media Privacy and Consumer Rights Act (S. 189) (continued)

-- to maintain and publish a description of their privacy and data security program, including who would have access to users' personal data and for what purposes and how privacy risks of new products will be addressed;

-- to provide consumers, upon request, with a copy of their personal data and a list of persons who received the data from the operator, free of charge and in an easily accessible form;

-- to notify affected users of transfers of personal data in violation of the operator's privacy or data security policies within 72 hours of the company's becoming aware of the violation and provide options to prevent the company's further collection, use, storage, and/or sharing of the consumer's personal data; and

-- to audit their privacy and data security program every two years.

- Many of the bill's requirements would not apply to the development of "privacy-enhancing technology."
- The FTC, state attorneys general, and other state consumer protection officials could enforce the law; the FTC's authority would extend to nonprofit organizations and common carriers.

Federal Bills

Data Care Act (S. 3744)

Current status: Introduced by Sen. Schatz (D-HI) and 14 other Democratic Senators in December 2018, the bill has not been re-introduced in the current congressional session.

Key provisions:

"Online service providers," defined as entities "engaged in interstate commerce over the internet or any other digital network" and that "in the course of business, collect[] individual identifying data about end users," would be required to fulfill fiduciary duties of care, loyalty, and confidentiality.

- **Duty of care** would require service providers to "reasonably secure individual identifying data from unauthorized access" and promptly notify affected end users of a breach of that duty.
- **Duty of loyalty** would prohibit a service provider from using individual identifying data or data derived from individual identifying data to benefit the service provider to the detriment of an end user and that would result in reasonably foreseeable and material physical or financial harm to an end user or would be unexpected and highly offensive to a reasonable end user.
- **Duty of confidentiality** would prohibit service providers from disclosing or sharing individual identifying data except as consistent with the duties of care and loyalty; require the service provider to enter into a contract with the recipient imposing on the recipient the same fiduciary duties; and require the service provider to audit the practices of the recipient to ensure its fulfillment of the duties.

Federal Bills

Data Care Act (S. 3744) (continued)

- FTC would be given rulemaking authority to exempt categories of online service providers from the law—considering the privacy risks based on such factors as size, complexity and nature of offerings, and sensitivity of consumer information handled and the costs and benefits of coverage—and to create more detailed breach notification requirements.
- FTC, state attorneys general, and state consumer protection officials would have enforcement authority; the FTC's authority would extend to nonprofit organizations and common carriers.
- Preemption:
  - The bill explicitly states that it would not preempt state laws or regulations (or supersede other federal laws or regulations).

Federal Bills

Consumer Data Protection Act

Current status: Sen. Wyden (D-Or) released a discussion draft in November 2018. The bill has not yet been introduced.

Key provisions:

- "Covered entities" would be defined as persons, partnerships or corporations over which the FTC has jurisdiction and which:
  - Had at least $50 million in average annual gross receipts for the three prior years;
  - Had personal information on at least 1 million consumers and 1 million consumer devices; and
  - Was a data broker or other, similar, commercial entity that access to the information.

Federal Bills

Consumer Data Protection Act (continued)

- FTC would be given rulemaking authority to define and enforce: reasonable cybersecurity and privacy practices and procedures, consumer access and correction rights for stored personal information, and disclosure to consumers of third parties with whom data is shared.
- Covered entities that have not less than $1 billion in annual revenue and that collect, store, or use personal information on more than 1 million consumers or consumer devices or ones that collect, use, or store personal information of more than 50 million consumers or consumer devices would be required to submit to the FTC annual data protection reports—certified to by their CEO and Chief Information Security Officer (CISO)—describing in detail how they were in compliance with regulations issued by FTC.

Questions?

Jonathan G. Cedarbaum
(202) 663-6315
Jonathan.Cedarbaum@wilmerhale.com