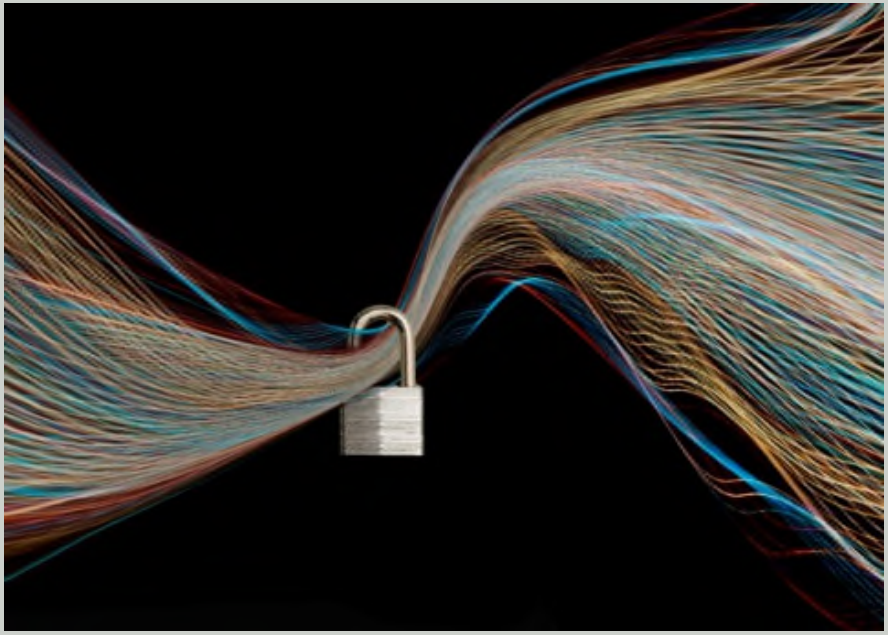
Ballard Spahr LLP

Understanding the California Consumer Privacy Act of 2018



Taylor Steinbacher
steinbachert@ballardspahr.comr
ogersmk@ballardspahr.com

Speakers

Taylor Steinbacher

Taylor is an associate in Ballard Spahr's Business and Finance practice group. His practice focuses on advising businesses, including banks, credit card issuers, and marketplace lenders, in matters regarding compliance with federal and state consumer protection statutes, including the Telephone Consumer Protection Act (TCPA), the Fair Debt Collection Practices Act (FDCPA), the Fair Credit Reporting Act (FCRA), the Truth In Lending Act (TILA) and Regulation Z, the CAN-SPAM Act, UDAAP/UDAP statutes prohibiting unfair, deceptive, and abusive acts and practices, state laws regarding retail installment sales contracts, and state usury laws.

He also counsels clients on privacy and data security matters such as data breaches/incidents and cross-border data transfers. He is accredited by the International Association of Privacy Professionals as a Certified Information Privacy Professional/United States (CIPP/US).

Roadmap

- **Other relevant California laws**
- **Discussion of privacy rights in statute**
- **Discussion of enforcement provisions**
- **GDPR comparison**
- **What businesses should do now**

Other Relevant California Laws

Other Relevant California Laws

- **Cal. Bus. & Prof. Code § 22575**
  - Online Privacy Protection Act of 2003
- **Title 1.81 – Customer Records (§ 1798.80 - § 1798.84)**
  - § 1798.81 – Reasonable steps for disposal of customer records
  - § 1798.81.5 – Security procedures and practices
  - § 1792.82 – Notification of breach of security system
  - § 1792.83 – Shine the Light Law
  - § 1798.83.5 – Commercial Online Entertainment Employment Service Providers
  - § 1798.84 – Penalties
- **Title 1.81.5 – California Consumer Privacy Act of 2018**

Other Relevant California Laws

➢ Online Privacy Protection Act of 2003 (Cal. Bus. & Prof. Code § 22575)

- Operators of commercial websites or online services that collect "personal identifying information" must conspicuously post online privacy policies that:

1. Identify the categories of personal information collected and the categories of third parties to whom the information may be shared;
2. If applicable, describe the process used to review and request changes to any individual's personally identifiable information;
3. Describe how they notify consumers who use or visit the site or online service of material changes to the privacy policy;
4. Identify the policy's effective date;
5. Disclose how they respond to web browser "do not track" signals; and
6. Disclose whether other parties may collect personally identifiable information about an individual consumer's online activities over time and across different web sites when a consumer uses the web site or service.

Other Relevant California Laws

- **California Shine the Light Law (Cal. Civ. Code § 1798.83)**
  - Businesses with an established "business relationship" with a California resident that have, within the preceding calendar year, disclosed "personal information" to a third party, which the third party used for "direct marketing purposes" shall, upon request, provide (1) a list of the categories of personal information disclosed to third parties and (2) the name and address of all third parties that received the personal information
  - Covers 27 categories of personal information
  - Option to add "Your Privacy Rights" or "Your California Privacy Rights" links on business homepage or to homepage's link to business's privacy notice with description of rights under law and contact information for requests
  - Businesses that have an online privacy policy that allow users to opt in or opt out of information sharing are exempt

Other Relevant California Laws

- **California Shine the Light Law**
  - Private Right of Action (Cal. Civ. Code § 1798.84)
    - Fines of $500 per violation or $3,000 per violation if violation is willful, intentional or reckless plus attorneys' fees and costs
    - Safe harbor if business provides information within 90 days of when it knew it failed to provide the information (unless the violation was willful, intentional or reckless)

Other Relevant California Laws

- **Information Security Statute (Cal. Civ. Code § 1798.81.5)**
  - "A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."
  - "A business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party that is not subject to subdivision (b) shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."
  - Covers six categories of personal information

Other Relevant California Laws

- **Disposal of Customer Records (Cal. Civ. Code § 1798.81)**
  - "A business shall take all reasonable steps to dispose, or arrange for the disposal, of customer records within its custody or control containing personal information when the records are no longer to be retained by the business by (a) shredding, (b) erasing, or (c) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means."
- **Data Breach Notification Statute (Cal. Civ. Code § 1798.82)**
  - Person or business that conducts business in California and that owns or licenses "personal information" shall disclose a breach of such information to California residents
  - Covers seven categories of personal information
  - Allows for private right of action

Background on Enactment of the CCPA

Background

Introduced & passed in 7 days

Which Entities are Subject to the CCPA?

Which Entities are Subject to the CCPA?

For-profit businesses doing business in California

[*one or more of the following*]

Annual gross revenues > $25 million	Personal information of ≥ 50,000 consumers, households, or devices	Sale of Personal information accounts for ≥ 50% of annual revenues

Explanation of the Consumer Rights Provided in the CCPA

Ballard Spahr LLP

Who Holds the Rights Afforded Under the CCPA?

- California residents
  - Every individual in California for other than a temporary or transitory purpose, and
  - Every individual who is domiciled in California who is outside the State for a temporary or transitory purpose

What Information is Protected?

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

- Biometric data
- Geolocation data
- Browse and search history
- Purchase history or tendencies
- Interactions with ads and apps
- Education information
- Employment-related information
- **Inferences drawn from such information**

Consumer Rights Provided in the CCPA

- Right to information
- Right to be forgotten
- Right to opt out of sharing with third parties
- Right to equal service
- Right to data portability (kind of)

Consumer Right to Request Information from . . .

. . . Businesses that "collect" personal information

- Categories of PI collected about that consumer
- Categories of sources from which the PI was collected
- Business purpose for collecting or selling the PI
- Categories of third parties with whom the PI was shared
- Specific pieces of PI collected about that consumer

. . . Businesses that "sell" personal information

- Categories of PI collected about that consumer
- Categories of PI sold and the categories of third parties to whom it was sold
- Categories of PI disclosed about that consumer

Definition of "Business Purpose"

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

Examples of Business Purposes Identified in Statute	
Maintaining or servicing accounts	Providing customer service
Processing or fulfilling orders and transactions	Verifying customer information
Counting ad impressions to unique visitors	Auditing related to a current interaction with the consumer
Detecting security incidents	Processing payments
Providing financing	Providing advertising or marketing services
Providing analytic services	Undertaking internal research for technological development and demonstration

Responding to Requests for Information

- At least two methods for consumers to submit requests
- Provide requested information within 45 days
  - Can get one 45-day extension when "reasonably necessary"
- Disclosure must cover the preceding 12-month period
- Must be free of charge

Method of Disclosure/Data Portability

1798.100(d)

- By mail
- Electronically
  - Portable
  - Readily usable format

Consumer Right to Request to be Forgotten

- Business must delete PI from its records and direct any service providers to do the same

Nine Exceptions:

- Necessary to provide good or service requested by consumer
- Scientific, historical, or statistical research (GDPR-like)
- Enable solely internal uses "reasonably aligned" with the expectations of the consumer
- Use internally in a lawful manner compatible with the context in which the consumer provided the PI

Consumer Right to Opt Out

- Right, at any time, to direct a business not to sell that consumer's PI to any third parties
- Express authorization required to sell thereafter

Enhanced Rights for Minors

- Under 16 years of age – "right to opt in"
- Willful disregard of a consumer's age deemed actual knowledge of consumer's age

Consumer Right to Equal Service

Businesses are prohibited from:

- Denying goods or services
- Charging or providing a different price, rate, level, or quality of goods or services, or suggesting same

UNLESS the difference is "*reasonably related*" to the value provided to the consumer by the consumer's data

- Financial Incentive Programs are permitted if that difference is "*directly related*"

Employee Training

All "individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance" must be informed of:

1. All of the rights provided in the Act; and

2. How to direct consumers to exercise their rights

Online Privacy Policy Requirements

Ballard Spahr LLP

Online Privacy Policy Requirements

- **Businesses must disclose the following in their online privacy policy and in any California-specific privacy rights description:**
  - **Description of Rights:**
    - Describe right to request that business provide information about personal information that it collects
    - Disclose right to request deletion of personal information
    - Describe anti-discrimination rights
    - Describe one or more methods for submitting requests

Online Privacy Policy Requirements

- **Lists of Categories of Personal Information:**
  - Lists the categories of personal information that business has (in the preceding 12 months):
    - collected about consumers
    - sold about consumers (or state that business has not sold consumer personal information)
    - disclosed about consumers for a business purpose (or state that business has not disclosed consumer personal information)
- **Duty to Update:**
  - Information must be updated at least once every 12 months

Online Privacy Policy Requirements

- Businesses that sell personal information and are required to comply with § 1798.120 (opt-out provision) must also:
- **Homepage:**
  - Provide a "clear and conspicuous link on the homepage titled "Do Not Sell My Personal Information" that allows consumers to go to a web page and exercise their opt-out rights
- **Privacy Notice:**
  - Include a description of opt out right and a link to the "Do Not Sell My Personal Information" web page in privacy notice and in any California-specific description of privacy rights

Online Privacy Policy Requirements

- **Exception:**
  - Businesses do not have to make links and texts available to non-California residents if they:
    1. Maintain a separate and additional homepage that is dedicated to California consumers and
    2. Take "reasonable steps" to ensure that California consumers are directed to that homepage

Rights Given to Businesses

Rights Given to Businesses

- **Additional Time to Respond**
  - Business can take an additional 45 days to respond to a verified request if business notifies consumer within the initial 45 day period and provides reasons for the delay. § 1798.130(2)
    - *But see* § 1798.145(g) ("up to an additional 90 days")
- **Right Not to Act**
  - Business can charge a reasonable fee or refuse to act on the request if the request is "manifestly unfounded or excessive." § 1798.145(i)
  - If business does not take action on the request it must inform the consumer within the time period permitted for its response of reasons for not taking action and any appeal rights. § 1798.145(h)

Exclusions

Exclusions

- **Legal Exclusions**
  - Law does not restrict business's ability to:
    - Comply with federal, state or local laws
    - Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities
    - Cooperate with law enforcement agencies
    - Exercise or defend legal claims

Exclusions

- **Deidentified or Aggregate Consumer Information**
  - Law does not restrict business's ability to collect, use, retain, sell or disclose consumer information that is deidentified or aggregated
    - "Deidentified" and "aggregate consumer information" are defined terms
- **Collection/Sale Occurs Entirely Outside California**
  - Law does not apply to collection or sale of consumer's personal information if every aspect of that takes place outside of California
  - Business cannot store information while consumer is in California and wait to collect it when consumer leaves California

Exclusions

- **HIPAA PHI Carve Out:**
  - Act "shall not apply to protected or health information that is collected by a covered entity governed by the Confidentiality of Medical Information Act . . . or governed by the privacy, security, and breach notification rules issued by the federal Department of Health and Human Services . . . ."
- **Consumer Reporting Agency Carve Out:**
  - Act "shall not apply to the sale of personal information to or from a consumer reporting agency if that information is to be reported in, or used to generate, a consumer report . . . and use of that information is limited by the federal Fair Credit Reporting Act"
- **Financial Institutions:**
  - "This title shall not apply to personal information, collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act . . . and implementing regulations, if it is in conflict with that law."

Third Parties and Service Providers

Third Party v. Service Provider

- **Privacy rights provided in CCPA refer only to third parties, not service providers:**
  - Business must disclose the categories of third parties with whom the business shares personal information. § 1798.110(a)(4)
  - Business that sells personal information must, upon request, disclose the categories of third parties to whom the consumer's personal information was sold. § 1798.115(2)
  - Business must provide notice to consumers that it sells personal information to third parties. § 1798.120(b)
  - Consumer has the right to opt out of business selling consumer personal information to third parties. § 1798.120(a).

Definition of Third Party

- Means a person who is *not* any of the following:

1. A business.

2. A person to whom the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract:

- (A) Prohibits the person receiving the personal information from:
  - (i) Selling the personal information.
  - (ii) Retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract.
  - (iii) Retaining, using, or disclosing the information outside of the direct business relationship between the person and the business.
- (B) Includes a certification made by the person receiving the personal information that the person understands the restrictions in subparagraph (A) and will comply with them.

Service Providers

- For profit legal 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."

Service Providers

- **Subject to Right to be Forgotten**
  - Businesses that receive a verifiable request to delete a consumer's personal information must also ensure that service providers delete the consumer's personal information from their records. § 1798.105(c)
  - Notably, third parties are not included in right to be forgotten

Service Providers

- **Liability:**
  - A business that discloses personal information to a service provider cannot be held liable if the service provider uses it in violation of the Act if at the time of disclosure the business did not have actual knowledge, or reason to believe, that service provider intended to commit the violation. § 1798.145(h)
  - Service providers can be subject of Attorney General enforcement actions even though their obligations are limited under the Act
- **Caveat:**
  - Definitions of "business" and "service provider" do not exclude the other term

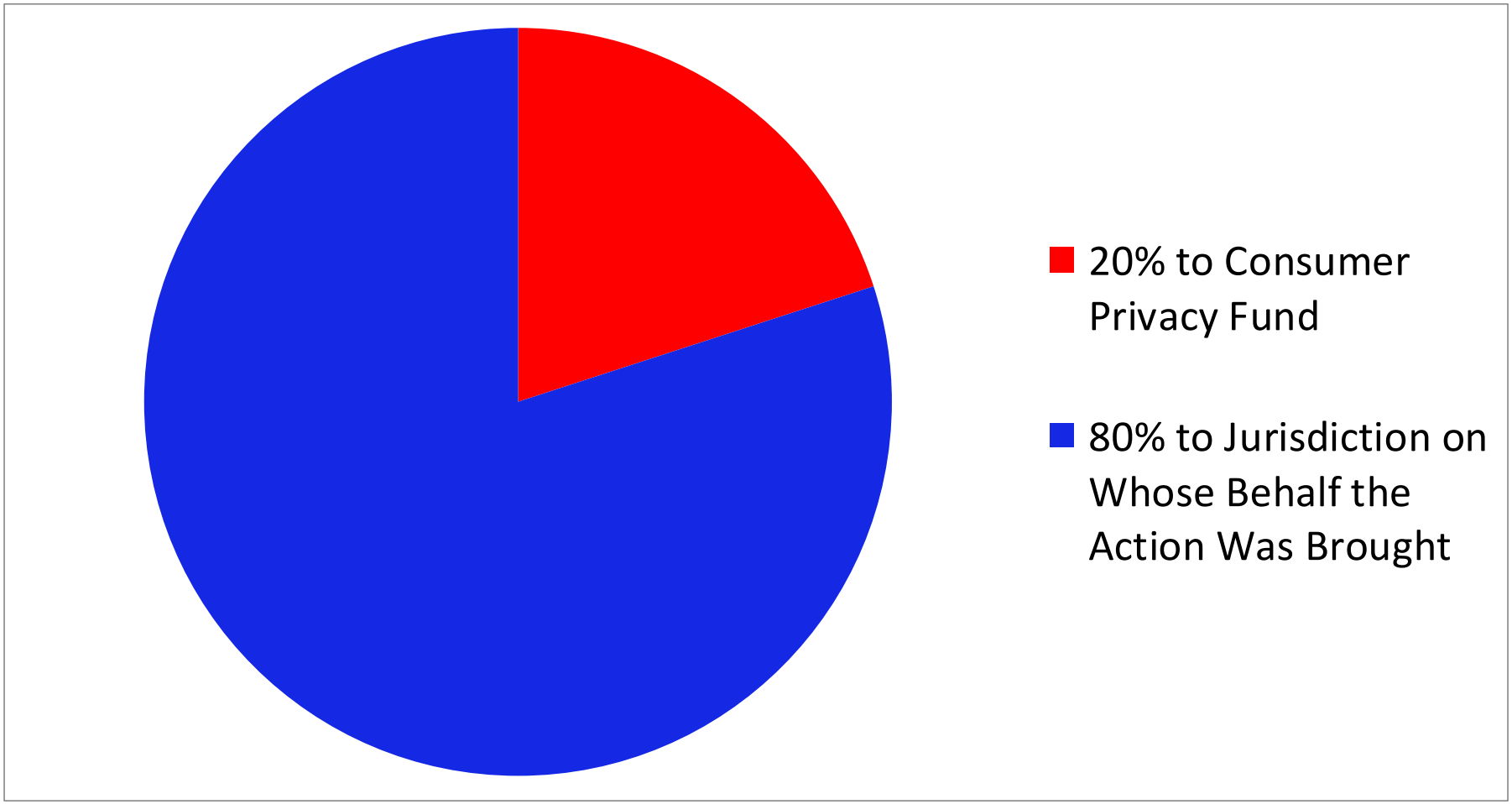
Enforcement Provisions

Civil Penalties – AG Enforcement

- Violation: A business shall be in violation of this title if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance.

- Damages: $2,500 per violation
  or
  $7,500 per intentional violation

Allocation of Enforcement Penalties



Private Right of Action

Private Right of Action – Data Breach Only?

1798.150. (a) (1) Any consumer whose nonencrypted or 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' 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:

Private Right of Action – Data Breach Only?

1798.150. (a) (1) Any consumer ~~of a business whose personal information~~ *whose nonencrypted or nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5,* is subject to ~~a security breach of the business as described in Section 1798.82 as~~ *an unauthorized access and exfiltration, theft, or disclosure as* a result of the business' 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:

Private Right of Action – Data Breach Only?

1798.150. (a) (1) Any consumer whose nonencrypted or 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' 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:

Private Right of Action – Standing

California Consumer Privacy Act:

1798.150. (a) (1) Any consumer whose nonencrypted or 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' 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:

Shine the Light / Breach Notification Laws:

(b) Any customer injured by a violation of this title may institute a civil action to recover damages.

Private Right Remedies

(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.

(2) In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.

Procedure for Action for Statutory Damages

30 Days' Notice to Business with Opportunity to Cure

↓

If Not Cured, May Bring Action

↓

Notify Attorney General Within 30 days

↓

30 Days for AG: (1) Notify of Intent to Take Case
(2) Refrain from Acting
(3) Order Consumer to Stop Action

Lessons from Prop 65

- Requires specific warnings for products that contain any of approximately 900 chemicals
- Private individuals can bring enforcement actions with similar AG "takeover" provision
- Nearly 700 settlements in 2017 alone
  - Over $25 million in settlement payments
  - Nearly $20 million in attorneys' fees

Attorney General Regulations/Guidance

Attorney General Regulations/Guidance

- Individualized/specific guidance from AG
- AG must "solicit broad public participation to adopt regulations" on or before January 1, 2020

Public Solicitation Requirement

- "Updating as needed additional categories of personal information . . ."
- "Establishing any exceptions necessary to comply with state or federal law . . . within one year of passage of this title and as needed thereafter."
- "Establishing rules and procedures . . . within one year of passage of this title and as needed thereafter . . . To govern compliance with a consumer's opt-out request."
- "The Attorney General may adopt additional regulations as necessary to further the purposes of this title."

Comparison of GDPR v. CCPA Privacy Rights

Ballard Spahr LLP

GDPR v. CCPA Privacy Rights

	GDPR	CCPA
Who it applies to	Organizations holding personal data of EU citizens. Art. 3	For-profit entity that (1) collects California consumers' personal information; (2) does business in California and (3) (a) has annual gross revenues in excess of $25,000,000; (b) buys, receives, sells or shares for commercial purposes the personal information of 50,000 or more California consumers, households or devices; or (c) derives 50% or more of its annual revenues from selling California consumers' personal information.

GDPR v. CCPA Privacy Rights

	GDPR	CCPA
Consent Mechanism	Opt in. Art. 6 ("data subject has given consent to the processing of . . . personal data for one or more specific purposes"); Art. 7	Opt out (of sale of personal information to third parties). § 1798.120(a)
Entities must provide certain information to individuals	Yes. Art. 13 (requires disclosure of specific information such as purposes of processing, contact information, and existence of certain rights under GDPR)	Yes. § 1798.130(5) & § 1798.135 (entities must disclose certain information in online privacy policies, including description of California-specific consumer rights and provide link for opt-out requests

GDPR v. CCPA Privacy Rights

	GDPR	CCPA
Right to obtain access to personal data	Yes. Art. 15	Yes. § 1798.100(a) (right to know what categories and specific pieces of personal information are collected)
Right to rectification / correction	Yes. Art. 16	No.
Right to be forgotten	Yes. Art. 17	Yes. § 1798.105(a) ("consumer shall have the right to request that a business delete any personal information about the consumer")

GDPR v. CCPA Privacy Rights

	GDPR	CCPA
Right to object to processing of personal data by receiving entity	Yes. Art. 18; Art. 21	No.
Right to data portability	Yes. Art. 20	Yes. § 1798.100(d)
Right to be informed of sharing with third parties	Yes. Art. 15(1)(c)	Yes. § 1798.110(a)(4) (right to request that business identify the "categories of third parties with whom the business shares personal information"); § 1798.115 (a)(1) (right to request categories of PI that business sold about consumer and categories of third parties to whom PI was sold)

GDPR v. CCPA Privacy Rights

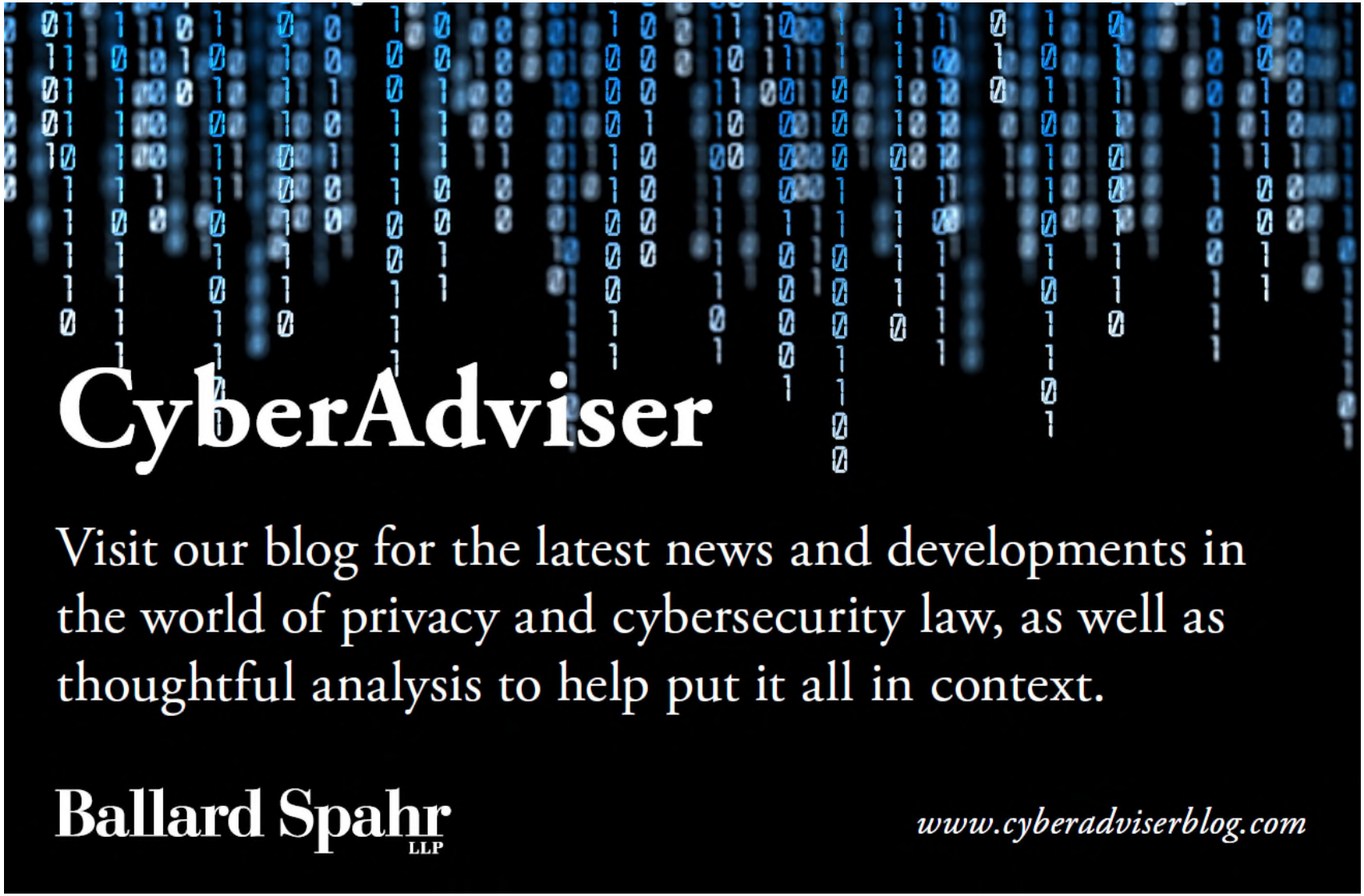
	GDPR	CCPA
Right to opt out of sharing of data with third parties	Yes. Art. 6 (requires opt in consent)	Yes. § 1798.120(a) ("A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information").
Anti-Discrimination Provision	No.	Yes. § 1798.125(a)(1) ("A business shall not discriminate against a consumer because the consumer exercises any of the consumer's rights")

What Businesses Should Do Now

What Businesses Should Do Now

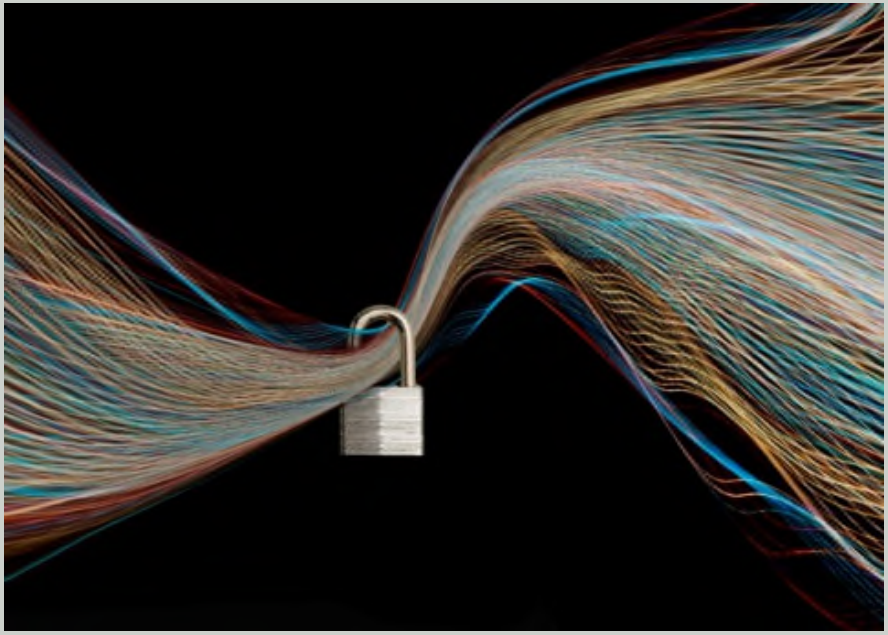
1. **Comply with Shine the Light Law**
2. **GDPR gap analysis**
3. **Develop compliance time frame**
4. **Data mapping**
5. **Use of deidentification and aggregation**
6. **Third-party vendor management**
7. **Review/revise relevant third party contracts**
8. **Provide comments to Attorney General's office**

Visit Our Blog – *CyberAdviser*



Ballard Spahr LLP

Understanding the California Consumer Privacy Act of 2018



Taylor Steinbacher
steinbachert@ballardspahr.comr
ogersmk@ballardspahr.com