



# Privacy Laws

Jonathan Nuechterlein & Alan Charles Raul  
Sidley Austin LLP

September 6, 2019

**SIDLEY**

TALENT. TEAMWORK. RESULTS.

# Substance and sources of law applicable to commercial actors

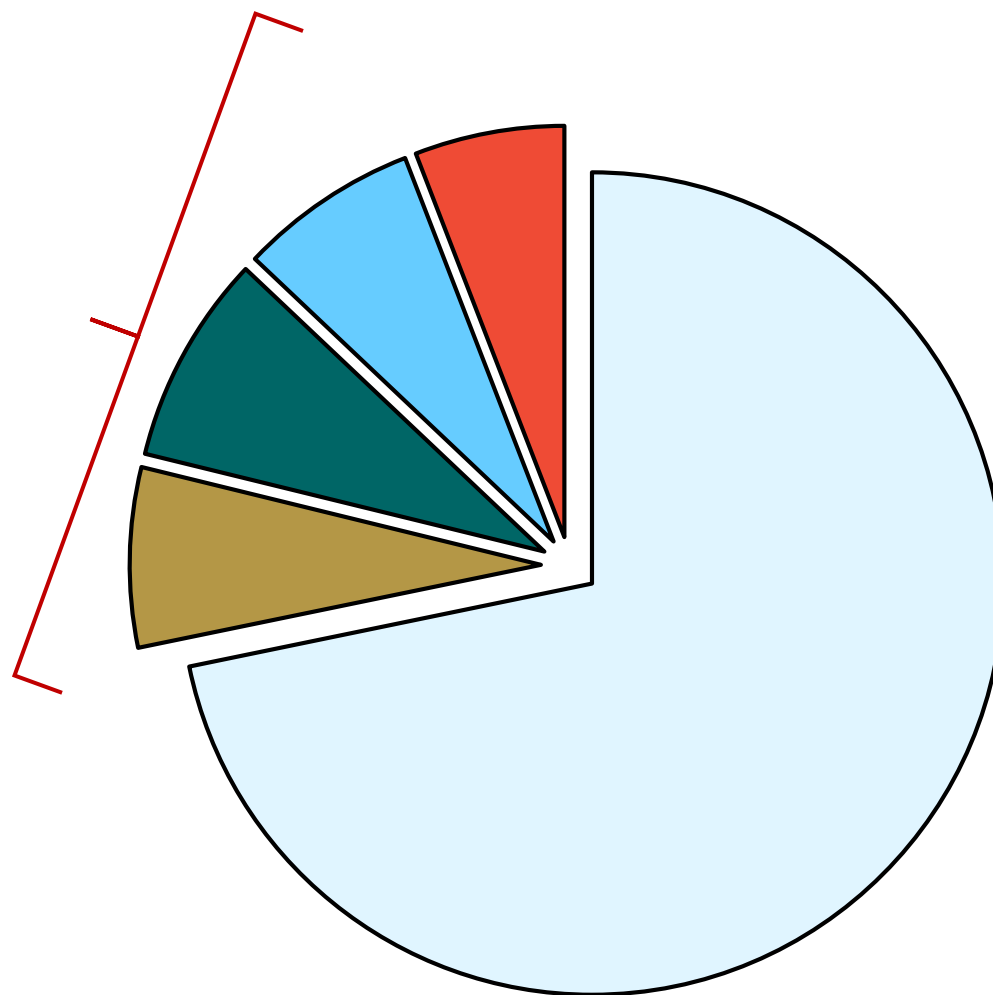
---

- Subject matter:
  - *Privacy*:
    - What is personally identifiable information, and how should it be collected, used, and shared?
  - *Data security*:
    - What measures must be taken to protect consumer data from unauthorized misuse?
  - *Data breach reporting*:
    - What steps must be taken to inform government authorities and affected consumers once a data breach occurs?
- Sources of law:
  - Federal
  - State/municipal
  - Foreign

# Federal privacy/data security statutes: a polyglot

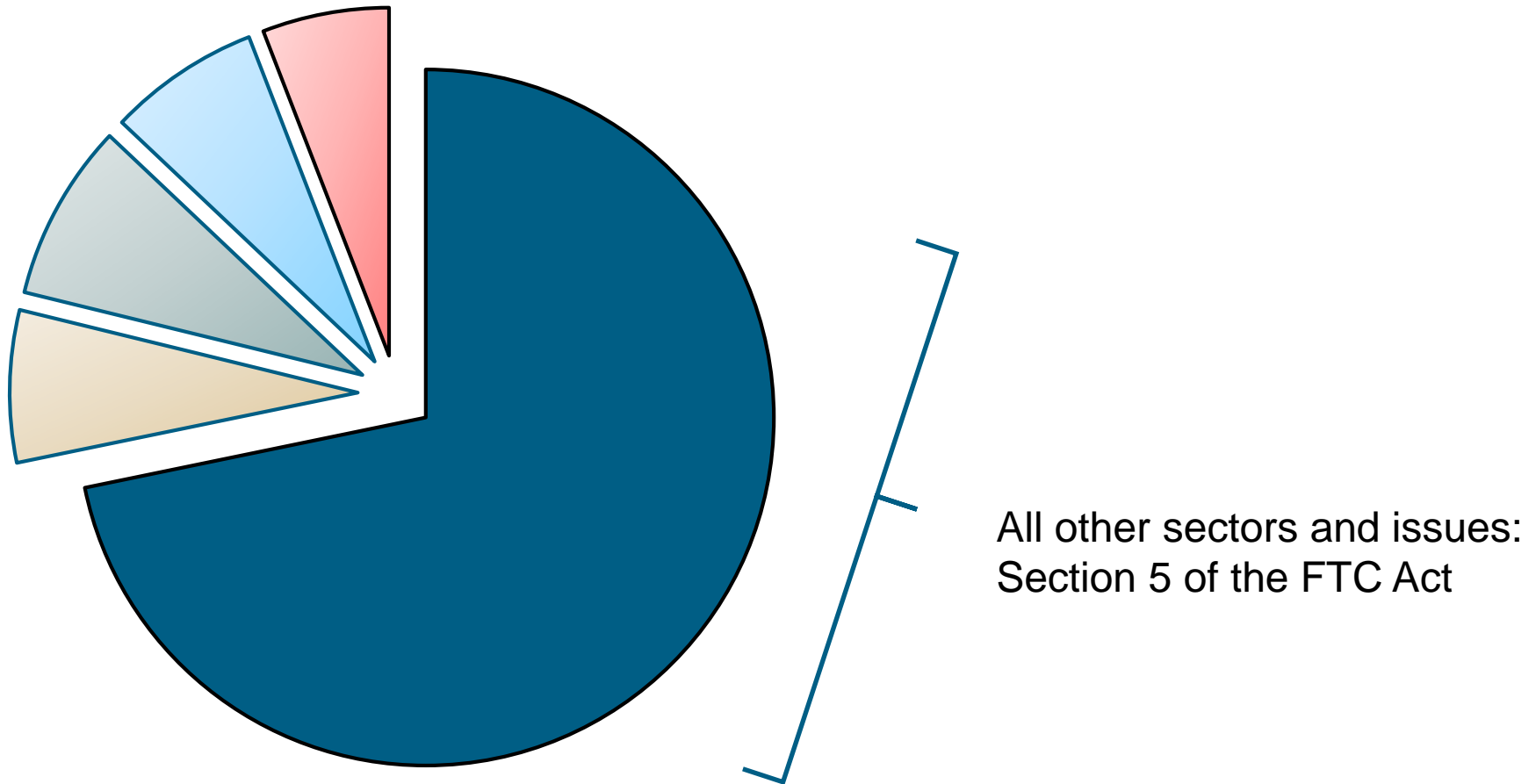
Sector-specific regulation governing commercial actors (a non-exhaustive list):

- Financial data (Gramm Leach Bliley; enforced by various agencies)
- Consumer credit data (FCRA; CFPB and FTC)
- Health data (HIPAA; HHS)
- Children's data (COPPA; FTC)
- Telecommunications services data (Communications Act; FCC)
- Electronic communications (ECPA; DOJ)
- Cable/satellite data (Cable and Satellite Acts; FCC)
- Student education data (FERPA; Dep't of Education)
- Etc.



## Federal privacy/data security statutes: a polyglot (cont'd)

---



## Section 5: overview

---

- Unlike EU law, the FTC Act uses a retrospective law enforcement model akin to the common law.
- Section 5 of the FTC Act prohibits “unfair or deceptive acts or practices in or affecting commerce.” 47 U.S.C. § 45(a).
- The FTC deems conduct “deceptive” if it involves misrepresentations or omissions of material information likely to mislead reasonable consumers.  
Representative FTC cases:
  - *Misrepresentation*: A company tells its customers that it will not sell personally identifiable data to third parties but then does so anyway.
  - *Omission*: A company offers a mobile app, identifies potential first-party uses of customer data, but fails to mention that the data will be shared with third parties.
- The FTC may deem conduct “unfair” if it “causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.” *E.g.*:
  - Company X takes unreasonably inadequate steps to protect its customers’ credit card data from cybersecurity threats, enabling hackers to obtain the data and harm the customers.

## Section 5: procedure, remedies, and new uncertainty

---

- Absent a settlement, the FTC can bring Section 5 cases either administratively (e.g., *LabMD*) or in federal district court (e.g., *Wyndham*).
- For pure Section 5 cases, the FTC typically sues in federal court if it wishes to recover “equitable monetary relief.”
  - Section 13(b) authorizes courts to issue “a permanent injunction” in “proper cases” where a defendant “is violating, or is about to violate,” the FTC Act. Starting in the 1980s, lower courts construed this language to permit disgorgement/restitution. But:
  - Intervening Supreme Court decisions draw that approach into question.
  - Citing those decisions, the Seventh Circuit (*Credit Bureau Center*) recently overruled its own precedent and held that Section 13(b) does *not* permit equitable monetary remedies, creating an explicit circuit conflict.
  - Even where such remedies remain legally available, they can be poorly tailored to privacy/data security cases.
- *Damages* are available only under section 19, and only where “a reasonable man would have known under the circumstances [that the conduct] was dishonest or fraudulent.”
- The FTC’s civil penalty authority is unavailable for Section 5 violations; it extends only to violations of specific FTC orders (including consent orders) or, in some cases, FTC rules.

# FTC notice-and-choice guidance

---

- The FTC has long endorsed a flexible approach to consumer privacy that targets potentially harmful uses of data but does not interfere with the beneficial uses that fuel the growth of the commercial internet.
- That flexibility is particularly evident in the FTC's approach to "notice and choice" issues, involving the mechanisms that businesses use to obtain or infer consent to particular data uses.
- Non-binding 2012 FTC *Privacy Report*: Context informs what firms can reasonably infer about consumer expectations.
  - "Most first-party marketing practices are consistent with the consumer's relationship with the business and thus do not necessitate consumer choice."
  - Consent mechanisms for data sharing with third parties (unrelated to the delivery of services or context of collection) depend on data sensitivity:
    - *De-identified/aggregated* data generally requires no consent mechanism.
    - Personally identifiable data in *sensitive* categories (e.g., medical or financial information) is generally subject to *opt-in* mechanisms.
    - Personally identifiable *non-sensitive* data is generally subject to *opt-out* mechanisms.
- Industry self-regulatory groups (e.g., DAA, DMA) have long played a central role in administering this regime.

# Foreign privacy laws

---

- US companies doing business abroad must consider their obligations under foreign as well as US law.
- The EU's General Data Protection Regulation ("GDPR"):
  - Is much more prescriptive than the FTC's Section 5 approach.
  - Establishes overbroad (and often ambiguous) limits on the collection, sharing, and use of consumer data. For example, GDPR:
    - Prohibits processing of personal data without a preexisting lawful basis (such as consent, contract, legal obligation, or "legitimate interest").
    - Requires opt-in consent mechanisms in a broad range of contexts involving "automated processing," even for uncontroversial uses of non-sensitive data. This inhibits, e.g., innovations in AI and in data analytics tools needed to detect cybersecurity events.
    - Imposes highly detailed notice requirements, resulting in privacy notices that are paradoxically more difficult for ordinary consumers to read and understand.
  - Regulates when and how data may be transferred between the EU and other jurisdictions (such as the US).
  - Imposes major financial penalties for violations.
- In the wake of GDPR, other major US trading partners (e.g., India) have begun considering EU-like privacy laws of their own.



# State data breach laws

---

- Apart from certain sector-specific laws, federal law imposes no specific requirements governing how companies must report and remediate data breaches.
- In contrast, all 50 states do have data-breach laws.
- Those laws vary in many different respects. *E.g.*,
  - Which entities are covered?
  - What types of breached information are covered?
  - What constitutes a “breach”: unauthorized *access* or unauthorized *acquisition*?
  - Does a breach need to threaten concrete harm before reporting is required?
  - How quickly must affected customers be notified?
  - Do state regulators need to be notified?
- Until very recently, state privacy/data security law generally focused *only* on these breach-notification requirements.
- But ...

---







## ***The Times They Are a-Changin'***



# The California Consumer Privacy Act

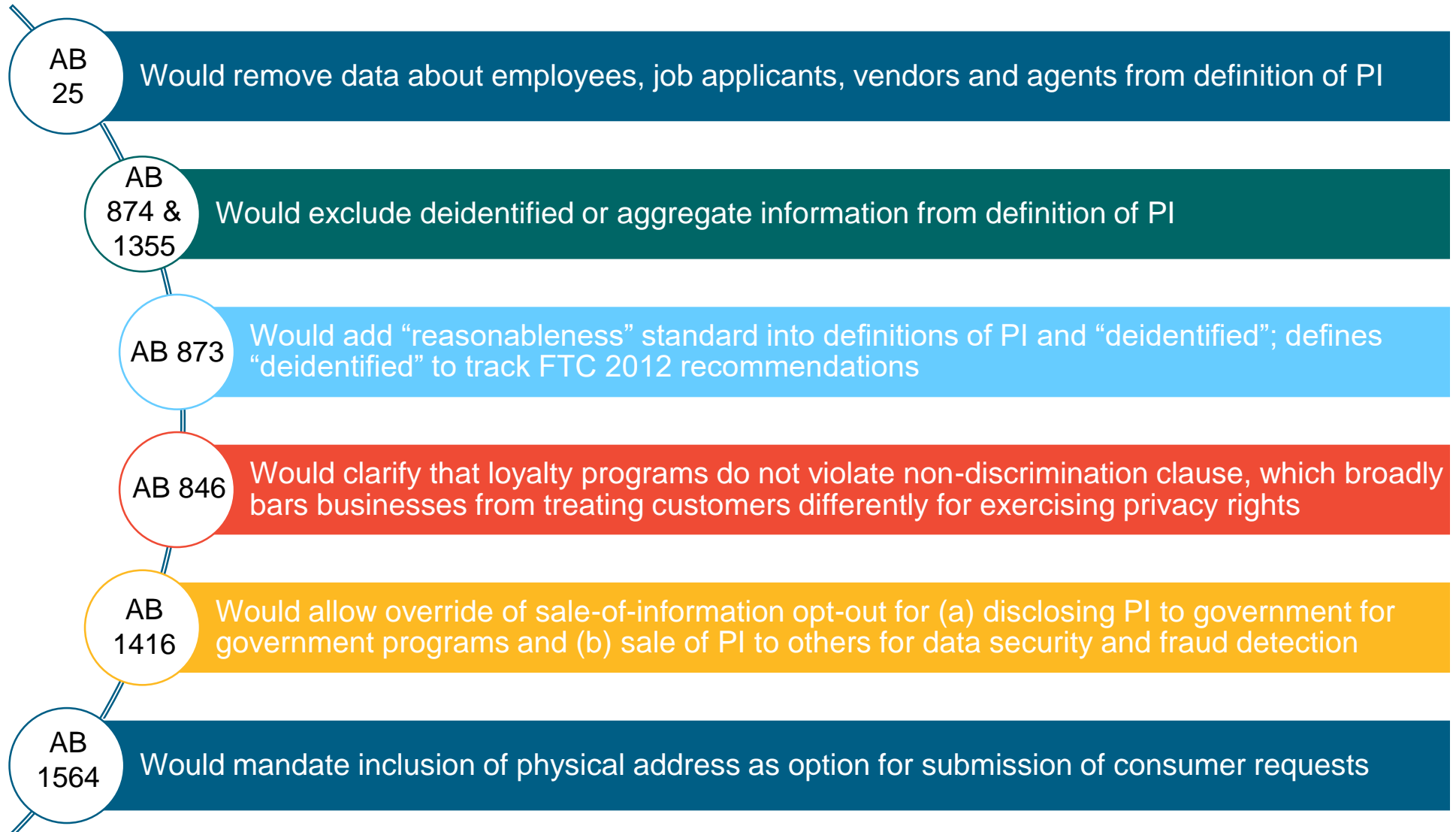
---

- The CCPA imposes far-reaching privacy and data-protection obligations on companies that “do business” in California.

	Adopted in 2018; will come into force Jan. 2020.		On request, companies must provide personal information they have collected about a customer and, with some exceptions, delete it.
	Applies to certain for-profit entities doing business in California and defines personal information very broadly.		Creates private cause of action for data breaches and authorizes damage awards without proof of harm.
	Broad privacy policy disclosure requirements.		Authorizes California Attorney General to enforce provisions with statutory fines.

- The CCPA was passed very quickly, in response to a ballot initiative.
- The California legislature has already amended it once to fix the most obvious problems, with more amendments anticipated.
- The California AG must then provide post-enactment regulatory guidance on the meaning of critical but ambiguous provisions.

# Relevant amendments in play

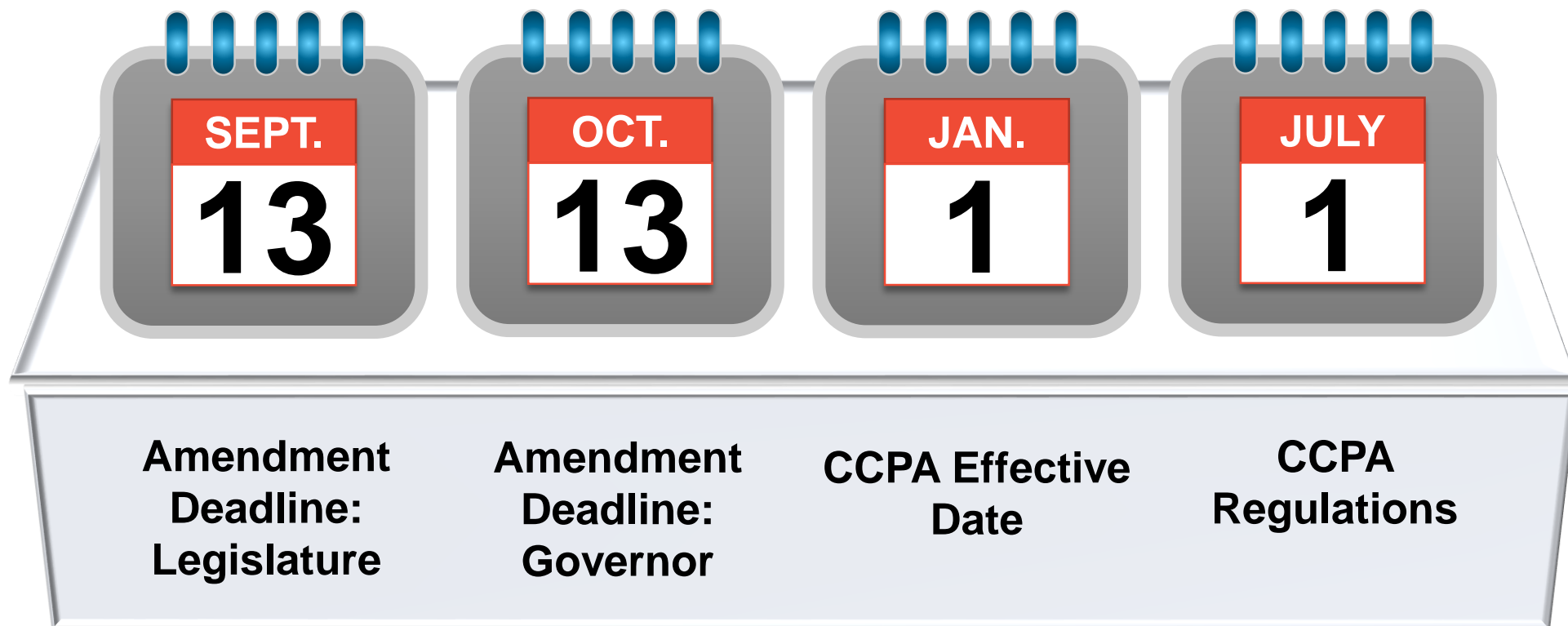


# California's GDPR? Key similarities and differences

Symbol					
Incremental CCPA Obligations Relative to GDPR					
⊘ Significant incremental obligations between CCPA and GDPR					
⚠ Certain key incremental obligations between CCPA and GDPR					
✔ Generally few incremental obligations between CCPA and GDPR					
Topic	Key CCPA Provisions	Key GDPR Provisions	Top-Line Comparison (Does Not Address Every Distinction)	Incremental CCPA Obligations Relative to GDPR	
<b>Threshold Conditions</b>					
<i>Effective date</i>	1 January, 2020	25 May, 2018	N/A		
<i>Covered entities</i>	§ 17 8.140(c) § 17 8.145	Article 3	Different territorial scopes: although, both the GDPR and the CCPA have broad scopes, the CCPA applies to profit organisations that collect or sell personal information (PI) on California residents while conducting business in California and includes various exceptions (e.g., certain small entities, specific industries).	⊘	
<i>Definition of covered information</i>	§ 17 8.140(o)	Article 4	Similar practical impact as the GDPR and the CCPA apply to PI: although, the CCPA explicitly applies to information associated with a "household", but there are specific exclusions such as for publicly available information.	✔	
<i>Inferred information</i>	§ 1798.140(o)(K)	Article 4 Article 22	Definitions similar, but the CCPA definition of PI includes "inferences drawn from" information to "create a profile about a consumer", while the GDPR's definition of personal data includes information that relates to an identified/identifiable individual.	⚠	
<i>Covered activities</i>	§ 17 8.140(e and t)	Article 2	GDPR appears broader as it applies to "processing" whereas, the CCPA is mainly focused on the "collection" and "sale" of PI.	⚠	
<i>Conditions for processing</i>	N/A	Articles 5(1)(e), 6(1)	The GDPR provides processing of personal data must be based on one of six grounds. <u>No directly comparable CCPA provision</u> although consumers may ask businesses not to sell their PI.	✔	
<b>Rights</b>					
<i>Responsibilities for Processors</i>	§ 17 8.140(d)	Article 28	<u>No directly comparable CCPA provision</u> although, third parties who buy PI cannot sell it without providing notice and opt-out. Also, businesses must disclose consumer PI pursuant to a written contract.	⚠	
<i>Notice</i>	§ 17 8.100(b) § 17 8.130 § 17 8.135(a)	Articles 12–14	<u>Substantial overlap</u> as both the GDPR and the CCPA require information be provided to individuals such as categories of personal data and purposes although, the specifics of compliance may differ and the CCPA expressly requires affirmative notice of the categories of PI to be collected.  <u>The CCPA has "Do Not Sell My Personal Information" labelling requirement.</u>	⊘	
<i>Right of access</i>	§ 17 8.100	Article 15 Article 20	<u>Largely the same</u> as both the GDPR and the CCPA provide a right of access although, the GDPR provides access to additional information and the compliance requirements and ability to charge may differ. Also, under the CCPA, right only applies to PI collected in the 12 months prior to request.	⚠	
<i>Right to be forgotten</i>	§ 17 8.105(a)	Article 17	<u>The GDPR is broader</u> , as although the right to be forgotten is similar, the exceptions are quite different.	⚠	
<i>Right to "opt out" for third-party sale</i>	§ 17 8.120(a)	Article 7	<u>Similar practical impact</u> , as although the GDPR does not have a provision which specifically addresses this issue, the ability to withdraw consent under the GDPR likely provides a similar right.	✔	
<i>Children</i>	§ 17 8.120(b)	Article 8	<u>Similar</u> although, the GDPR does not differentiate between ages 0–13 and 13–16 and relies on EU Member State law. The CCPA allows children's PI to be "sold" only on the basis of consent.	⚠	
<i>Non-discrimination</i>	§ 17 8.125	N/A	<u>No directly comparable GDPR provision</u> although, the practical implications of the CCPA are unclear. The CCPA provides consumers must not be discriminated because of the execution of their rights under the CCPA.	✔	
<b>Enforcement Provisions</b>					
<i>Rectification</i>	N/A	Article 16	The GDPR also provides data privacy rights of rectification, to object to processing and not be subject to automated processing, but there is <u>no directly comparable CCPA provision</u> .	✔	
<i>Right to object to processing</i>	N/A	Article 21			
<i>Right not to be subject to automated processing</i>	N/A	Article 22			
<i>Government Enforcement</i>	§ 1 98.155	Article 58 Article 83	The GDPR appears to be broader, with fines of up to 4% of global annual turnover and broader regulatory powers. Under the CCPA, civil penalties can be issued by a court which, depending on violation, can be \$2,500 for each violation or \$7,500 for each intentional violation. (NOTE: The CCPA enforcement funded by fines.)	⚠	
<i>Private Cause of Action</i>	§ 17 8.150	Article 77 Article 79	The GDPR appears to be much broader, with claims covering both material and non-material damages. The CCPA provides a powerful but limited cause of action, with statutory damages of at least \$100 per person.	⊘	
<b>Security and other Provisions</b>					
<i>Data Protection Officer (DPO)</i>	N/A	Articles 37–39	<u>No directly comparable CCPA provision</u> . The GDPR requires the appointment of a DPO in certain cases.	✔	
<i>Security Requirements</i>	N/A	Article 32	The GDPR requires controllers implement appropriate technical and organisational measures to ensure a level of security. <u>No directly comparable CCPA provision</u> , although California has a separate data security statute.	✔	
<i>Recordkeeping</i>	N/A	Article 30	The GDPR requires a controller to maintain a record of processing activities. <u>No directly comparable CCPA provision</u> .	✔	
<i>Breach Notification</i>	§ 17 8.150	Articles 33–34	The GDPR requires a controller to report a personal data breach without undue delay and, where feasible, not later than 72 hours after becoming aware of it. <u>No directly comparable CCPA provision</u> , although notification requirements exist in parts of California law.	⚠	

## Amendments and regulatory guidance

---



## Après California, le déluge?

---

- Nevada recently enacted privacy legislation with provisions similar to California's but distinct in several respects.
- Many other States are also considering broad privacy legislation, including New York, Washington, Connecticut, Massachusetts, New Jersey, Rhode Island, Utah, North Dakota, and Hawaii.
- Even some cities, including Chicago, are considering enactment of privacy ordinances with potentially nationwide effects.
- The likely result: a patchwork quilt of privacy obligations that vary greatly from state to state and even from city to city, defying the geography-agnostic nature of the internet.
- That hodgepodge is much more problematic for *privacy* regulation than for *data-breach reporting* requirements.
  - State-by-state variation in breach-reporting rules merely increases the number of lawyer hours needed to respond to a breach.
  - State-by-state variation in privacy regulation creates substantial regulatory uncertainty and impairs the efficiency of a company's underlying business.

# Prospects for federal privacy legislation

---

- There is broad agreement on the need for federal legislation.
  - A broad spectrum of interested parties from industry representatives to civil libertarians agree that new federal privacy legislation is needed.
  - Consumers and businesses would benefit from greater certainty and consistency in legal requirements.
- The positive aspects of the CCPA can be preserved, but also refined and improved.
  - The CCPA properly recognizes the value of privacy and the importance of standards that apply consistently across all industry sectors.
  - But federal legislation can establish easier-to-implement and nationally consistent standards establishing general consumer rights:
    - to know what data is collected about them and how it is used;
    - to control how such data is accessed or used; and
    - to be presented with opt-in or opt-out mechanisms for data-sharing with third parties, depending on context-specific variables such as data sensitivity.



# First principles for federal legislation

---

- Preserve innovation by avoiding excessively prescriptive requirements that cannot adapt to changing technologies (*cf.* GDPR and AI).
- Apply the same cost-benefit analysis the FTC has long applied to promote consumer interests while protecting data's role in fueling the information economy. *E.g.*, focus on genuine risks to consumers and distinguish between sensitive and non-sensitive data.
- Preserve the geography-agnostic nature of the internet by establishing national consistency in privacy rules.
- Vest primary implementation authority in the FTC and augment its funding to support its expanded role.
- To the extent that FTC rulemaking is needed in discrete contexts, authorize the FTC to employ standard APA procedures.
- Extend FTC civil penalty authority to appropriate privacy/data-security cases involving violations of Section 5.
- Authorize state AGs to play an enforcement role by bringing actions on behalf of their citizens (*cf.* state AG role under HIPAA and COPPA).
- Rely on these governmental authorities (rather than plaintiffs' lawyers) to enforce the terms of the legislation.

# Disclaimer

---

*This presentation has been prepared by Sidley Austin LLP and Affiliated Partnerships (the Firm) for informational purposes and is not legal advice. This information is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. All views and opinions expressed in this presentation are our own and you should not act upon this information without seeking advice from a lawyer licensed in your own jurisdiction. The Firm is not responsible for any errors or omissions in the content of this presentation or for damages arising from the use or performance of this presentation under any circumstances.*

Beijing  
Boston  
Brussels  
Century City  
Chicago  
Dallas  
Geneva  
Hong Kong  
Houston  
London  
Los Angeles  
Munich  
New York  
Palo Alto  
San Francisco  
Shanghai  
Singapore  
Sydney  
Tokyo  
Washington, D.C.



sidley.com