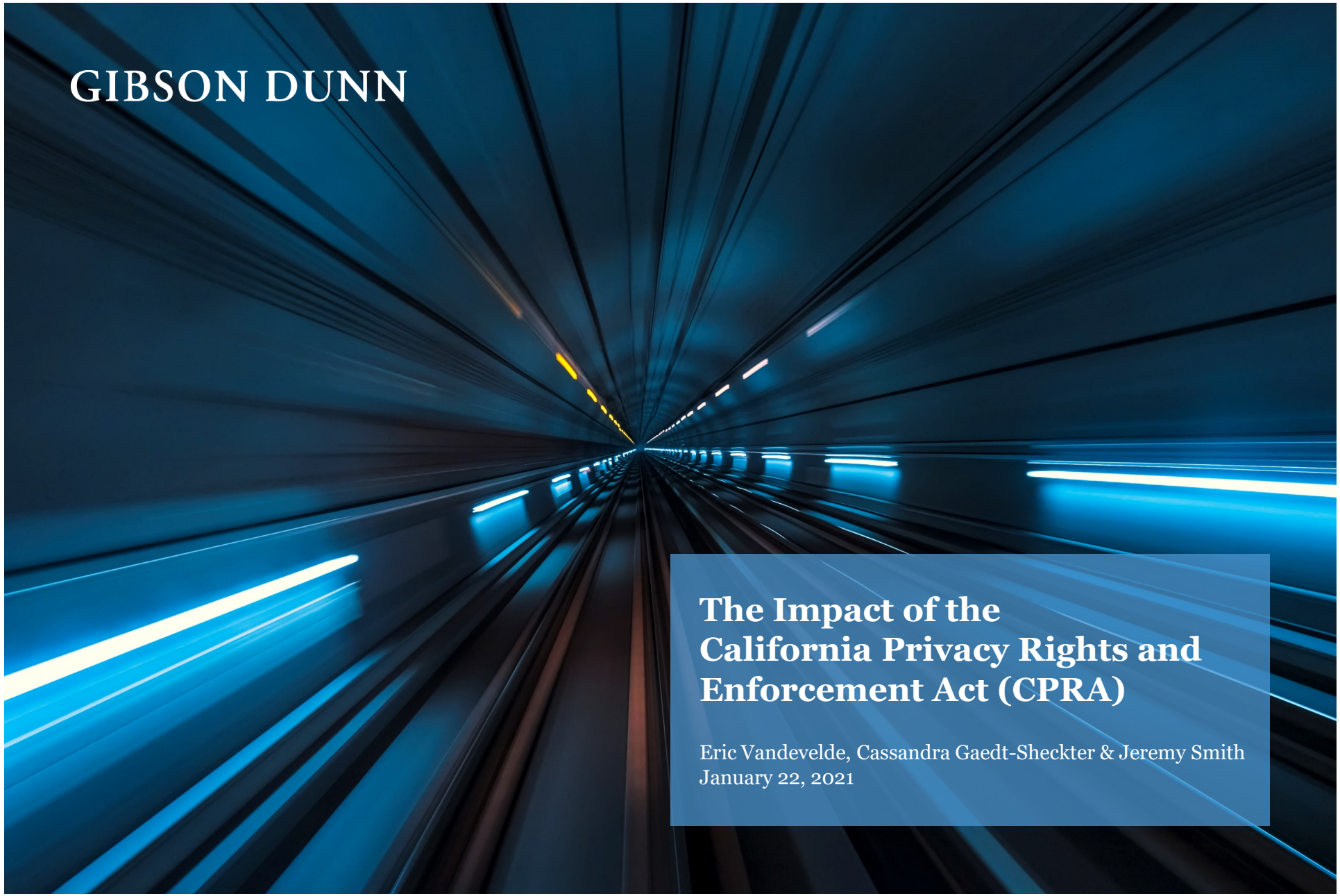


The Impact of the California Privacy Rights and Enforcement Act (CPRA)

Eric Vandevelde, Cassandra Gaedt-Sheckter & Jeremy Smith
January 22, 2021

Presenters

Eric D. Vandevelde, Partner in Los Angeles
evandevelde@gibsondunn.com
Eric is a former federal prosecutor and an experienced trial and appellate attorney. He has significant first-chair trial experience and a deep technical computer/software engineering background, having obtained a degree in Computer Science from Stanford University and worked as a software engineer in Silicon Valley and Latin America. From 2007 to 2014, Eric served as an Assistant U.S. Attorney in the U.S. Attorney's Office for the Central District of California. He was Deputy Chief of the Cyber & Intellectual Property Crimes Section, supervising one of the nation's largest teams of federal prosecutors dedicated to investigating and prosecuting computer hacking and intellectual property offenses.

Cassandra Gaedt-Sheckter, Of Counsel in Palo Alto
cgaedt-sheckter@gibsondunn.com
Cassandra's practice focuses on data privacy and cybersecurity litigation and counseling, complex technology litigation, and trade secret disputes. She has substantial experience advising companies on privacy and cybersecurity issues, including relating to legal and regulatory compliance with CCPA and CPRA—as one of the leads of the firm's CCPA/CPRA Task Force, GDPR, Children's Online Privacy Protection Rules (COPPA), and other federal, state, and international laws and regulations.

Jeremy S. Smith, Associate in Los Angeles
evandevelde@gibsondunn.com
Jeremy has represented clients in a wide range of litigation in both federal and state courts. He has defended clients in class actions across numerous substantive areas of law, including privacy, the Telephone Consumer Protection Act (TCPA), consumer fraud, and insurance law. Mr. Smith also represents clients on appeal in a wide range of matters, with a particular focus on appellate proceedings in California state court.

Today's Topics

1. CCPA 2.0: How did we get here?
2. CPRA Timeline
3. What's new? CPRA explained
4. Related and Additional Key Business Responsibilities
5. Class Actions and AG Enforcement

GIBSON DUNN

CCPA 2.0: How Did We Get Here?

How Did We Get Here?

Pre-June 2018: State claims require proof of injury; notification

June 2018: CCPA slated for 2018 ballot

June 2018: CCPA signed in new form by legislature

October 2019: Flurry of CCPA amendments passed

October 2019: First draft Attorney General's CCPA regulations

January 2020: CCPA takes effect

August 2020: Attorney General regulations take effect

November 2020: CPRA approved by California voters

January 2023: CPRA takes effect

Californians for Consumer Privacy Strike Back – California Privacy Rights Act

- Alastair Mactaggart (San Francisco Real Estate Investor) / Californians for Consumer Privacy proposed California Privacy Rights Act ("CPRA") as ballot initiative (aka Prop 24)
  - Same person / group that led the ballot initiative in 2016-2018 that resulted in the CCPA
- 8,665,716 California voters (56.1%) said "yes" to Prop 24

California Voter Sentiments

Pro Prop. 24

- Sense that CCPA was scuttled by legislature and subject to sectoral exemptions
  - "Unless California voters take action, the hard-fought rights consumers have won could be undermined by future legislation."
- Intent to correct AG enforcement bandwidth issues

Anti Prop. 24

- Key coalition members: ACLU, League of Women Voters, and California Nurses Association
  - CPRA does not go far enough
  - "Pay-for-Privacy" schemes (concern for discrimination)
  - Concern that employer-employee exceptions/delays were too favorable
  - Closed door scheme cooked up by "big tech"
    - Anticompetitive and onerous for smaller enterprises

CPRA Amendment Structure

- As a ballot initiative, Prop. 24 cannot be as easily amended.
- Prop. 24 argued that the California Legislature may be at odds with consumer privacy rights:
  - "Unless California voters take action, the hard-fought rights consumers have won could be undermined by future legislation." CPRA § 1(D).
- Amendments must be approved by further ballot, except arguments that if it strengthens privacy, it may be permissible.

CPRA Amendment Structure (cont'd)

- CPRA amendment/exemption limitation:
  - "The provisions of this act may be amended . . . if . . . **amended to enhance privacy and are consistent** with and further the purposes and intent of this act." CPRA § 25.
- This is a constitutionally permissible concept:
  - "When a court reviews Proposition 24 as a whole to ascertain the electorate's intent, it will find ample evidence of a plain intent to protect consumer privacy, to strengthen existing provisions, and to permit legislative amendments that provide even greater protection. To the extent that plain statement is unclear, a court will next examine the ballot materials." David A. Carrillo, *How California lives with two legislatures*, California Constitution Center (Aug. 5, 2020).
  - "This statement of intent unambiguously sets the floor and creates a one-way ratchet: the legislature can only amend this initiative by increasing privacy protections. Some opponents of Proposition 24 apparently argue that a legislative amendment of the law must satisfy *every* section of the law for it to be valid. That misstates the standard described above, and there is little danger a future court will use that approach . . . ." *Id.*

GIBSON DUNN

CPRA Timeline

California Privacy & Cybersecurity: Context

November 2020: CPRA approved by California voters
January 2022: "Look-back" period for CPRA begins
July 2022: CPRA regulation deadline
January 2023: CPRA takes effect
July 2023: CPRA becomes enforceable
January 2020 – January 2023: CCPA remains in effect

GIBSON DUNN

What's New? CPRA Explained

What's New?

- Core Concepts
  - Slight **narrowing of covered "businesses";** broadened "**publicly available**" definition
  - New concept of **"sensitive personal information"**
  - Expansion on concept of **"sharing"**
- New Rights for Consumers
  - **Limit use** of "sensitive personal information"
  - **Right to correct**
  - Expanded rights
    - Expanded **right to opt of "sharing"**
    - **Right of non-discrimination** expanded to employers

- Obligations for Businesses
  - Additional responsibilities vis-à-vis new rights (correction, sensitive personal information, etc.)
  - Data hygiene/minimization (including secondary use)
  - New notice and opt-out rules
  - Additional request to know obligations
  - Contract requirements for third parties (and other service provider obligations)
- Regulator
  - **California Privacy Protection Agency**
  - No more notice-and-cure procedure for administrative actions
  - NO expansion of private right of action

California Privacy Protection Agency

- New agency created
  - $10M annual budget for enforcement
  - Anticipated 20 person team
  - Will take on rulemaking and enforcement with the AG
- Administrative Fines
  - Similar to CCPA / AG but violations relating to minors will yield higher fine
  - $2,500 fines per violation. § 1798.199.55(a)(2).
  - $7,500 for intentional violations/minors. *Id*.

- Administrative Enforcement
  - Notice-and-cure procedure eliminated for administrative actions and made discretionary. § 1798.155(a).
  - Agency may consider lack of intent to violate the law or voluntary efforts to cure, when deciding whether to investigate a complaint or provide a business with time to cure. § 1798.199.45.

Applicability: Business Definition

- Clarification on how to count revenue
- Narrows scope of businesses, which may help smaller enterprises
  - "Business" defined as a for-profit business that:
    - "~~Has~~ As of January 1 of the calendar year, had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185." 1798.140(d)(1)(A).

    - "Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares ~~for commercial purposes, alone or in combination,~~ the personal information of ~~50,000~~ 100,000 or more consumers or, households~~, or devices~~." 1798.140(d)(1)(B).
    - "Derives 50 percent or more of its annual revenues from selling or sharing consumers' personal information." 1798.140(d)(1)(C).
- Broadens/clarifies the scope to include affiliates, joint ventures, and partnerships. 1798.140(d)(3).

Applicability: Affiliates

- Affiliates can also be considered a "business" (preexisting CCPA concept, clarified)
- Affiliate must (**1) receive personal information** and (**2) have common branding that would communicate common ownership to the average consumer**.
  - "Any entity that controls or is controlled by a business, as defined in paragraph (1), and that shares **common branding** with the business and with whom the business **shares** consumers' **personal information**. 'Control' or 'controlled' means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. 'Common branding' means a shared name, service mark, or trademark that the **average consumer would understand** that two or more entities are commonly owned." 1798.140(d)(2).

Applicability: Joint Ventures

- Joint ventures can also be a **considered a "business"** and thus subject to the CPRA.
- However, sharing of personal information among members of the joint ventures shall **not be considered to be "shared"** under the CPRA.
  - "A joint venture or partnership composed of businesses in which **each business has at least a 40 percent interest**. For purposes of this title, the joint venture or partnership and each business that composes the joint venture or partnership shall separately be considered a single business, except that **personal information in the possession of each business and disclosed to the joint venture or partnership shall not be shared with the other business**." 1798.140(d)(3).

Definition of "Personal Information" Narrowed

- Expands exclusion of "publicly available" information:
  - "'Personal information' does not include publicly available information *or lawfully obtained, truthful information that is a* ***matter of public concern***. For purposes of this paragraph, "publicly available" means*:* information that is lawfully made available from federal, state, or local government records*, or information that a business has a reasonable basis to believe is lawfully made available to the* ***general public*** *by the consumer or from widely distributed media, or by the consumer; or information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a* ***specific audience***. 'Publicly available' does not mean biometric information collected by a business about a consumer without the consumer's knowledge." 1798.140(v)(2).

Opt Out of Sale and Sharing

- **Right to opt-out** now applies to **both** (1) selling **and** (2) **sharing**
  - "A consumer shall have the right, at any time, to direct a business that sells or shares personal information about the consumer to third parties not to sell or share the consumer's personal information. This right may be referred to as the right to opt-out of sale or sharing." 1798.120(a).

- Creates **additional notification requirements:**
  - "Provide a clear and conspicuous link on the business's ~~Internet~~ Internet ~~homepage~~ homepages, titled "Do Not Sell or Share My Personal Information," to an ~~Internet~~ ~~Web~~ ~~page~~ internet web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale or sharing of the consumer's personal information." 1798.121(a)(1).

"Sharing" Definition Provided

- CPRA **adds definition** of "**sharing**" to clarify ambiguities related to definition of "**sale**" under the CCPA, in the context of cross-context behavioral advertising:
  - "'Share,' 'shared,' or 'sharing' means sharing, 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 a third party **for cross-context behavioral advertising**, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged." 1798.140(ah)(1).
- Cross-Context behavioral advertising:
  - "'Cross-context behavioral advertising' means the **targeting** of advertising to a consumer **based on the consumer's personal information** obtained from the consumer's **activity across businesses**, distinctly-branded websites, applications, or services, **other than the business**, distinctly-branded website, application, or service **with which the consumer intentionally interacts**." 1798.140(k).

Exclusions From "Sharing" Definition

- It is **not "sharing"** when:
  - "A **consumer uses or directs the business to intentionally disclose** personal information or intentionally interact with one or more third parties." 1798.140(ah)(2)(A).
  - Businesses communicate consumers' **opt out to others**. 1798.140(ah)(2)(B).
  - **As part of change in business control** (merger, acquisition, bankruptcy, *etc*.), but acquirer cannot "materially alter" how it uses the information, unless it provides sufficient notice. 1798.140(ah)(2)(C).

Sensitive Personal Information: Definition

- *New category, not contemplated by the CCPA, allowing consumers to "limit business use" of sensitive personal information.*
- Defined as:
  - "personal information' that reveals:

  - (A) A consumer's **social security, driver's license, state identification card, or passport number**.
  - (B) A consumer's **account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account**.
  - (C) A consumer's **precise geolocation**.
  - (D) A consumer's **racial or ethnic origin, religious or philosophical beliefs, or union membership**.
  - (E) The **contents of a consumer's mail, email, and text messages** unless the business is the intended recipient of the communication.
  - (F) A consumer's **genetic data**." 1798.140(ae)(1).
  - "**biometric information** [processed] for the purpose of uniquely identifying a consumer." 1798.140(ae)(2)(A).
  - "personal information collected and analyzed concerning a **consumer's health**[,]" "**sex life**[.]" or "**sexual orientation**." 1798.140(ae)(2)(B)-(C).

Sensitive Personal Information: Exclusions

- A **business' purpose** may downgrade it from **Sensitive Personal Information** to **Personal Information**:
  - "Sensitive personal information that is collected or processed **without the purpose of inferring characteristics about a consumer** is not subject to this section, as further defined in regulations adopted pursuant to subparagraph (C) of paragraph (19) of subdivision (a) of Section 1798.185, and **shall be treated as personal information** for purposes of all other sections of this act, including Section 1798.100." 1798.121(d).
- **Public information** is **not** **Sensitive Personal Information**:
  - "Sensitive personal information that is 'publicly available' pursuant to paragraph (2) of subdivision (v) shall not be considered sensitive personal information or personal information." 1798.140(ae)(3).

Sensitive Personal Information: GDPR v. CPRA

Information	GDPR	CPRA
Racial/ethnic origin	✓	✓
Political opinion	✓	X
Religious or philosophical belief	✓	✓
Union membership	✓	✓
Genetic, biometric	✓	✓
Health, sexual, sexual orientation	✓	✓
Government ID Nos. (SSN, DL, etc.)	X	✓
Account log-in information	X	✓
Financial information combined with access credentials	X	✓
Precise geolocation (equal or less than 1,850 feet + regs.)	X	✓
Contents of electronic communications	X	✓

Sensitive Personal Information: Consumer Rights and Business Responsibilities

- Consumers have a right to **limit use or disclosure** of "Sensitive Personal Information":
  - "A consumer shall have the right, at any time, to direct a business that collects sensitive personal information about the consumer to limit its use of the consumer's sensitive personal information **to that use which is necessary** to perform the services or provide the goods **reasonably expected by an average consumer** . . . ." 1798.121(a).
- Businesses **must**:
  - "Provide a **clear and conspicuous** link on the business' internet homepages, titled "Limit the Use of My Sensitive Personal Information . . . ." 1798.135(a)(2).
  - Provide **notice of other purposes/uses** of "sensitive personal information"
  - Follow consumer's requested limitations (refrain from selling or sharing) and don't ask again for 12 months (same as Personal Information sale opt outs under CCPA). 1798.135(b)(4)

Right to Correction

- *Another new concept for California* (but similar to GDPR right to rectification (Article 16)).
- Consumers can request **correction of "inaccurate" information:**
  - "A consumer shall have the right to request a business that maintains **inaccurate personal information** about the consumer to **correct** that inaccurate personal information, taking into account the **nature of the personal information and the purposes of the processing** of the personal information." 1798.106(a).
- Business must **disclose this right and use "commercially reasonable efforts"** to correct "personal information":
  - "A business that collects personal information about consumers **shall disclose**, pursuant to Section 1798.130, **the consumer's right to request correction** of inaccurate personal information." 1798.106(b).
  - "A business that receives a verifiable consumer request to correct inaccurate personal information **shall use commercially reasonable efforts to correct** the inaccurate personal information as directed by the consumer . . . ." 1798.106(c).

Right to Correction: Ambiguities

- A lot remains **unknown** with respect to "right to correction" and **will depend on regulations**:
  - How will "inaccurate" be defined or assessed?
  - Additional detail needed for how the nature of information and processing affects the request
  - Frequency of requests and response time in light of commercial reasonableness limitations

GIBSON DUNN

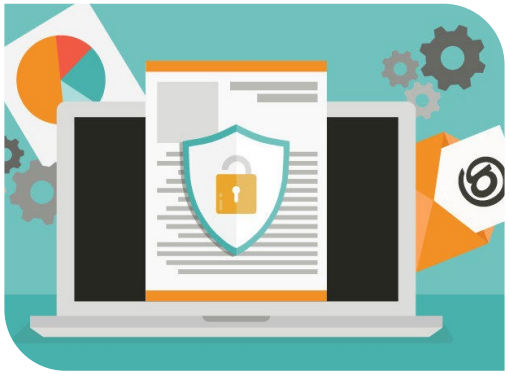
Related and Additional Key Business Responsibilities

Other Key Business Responsibilities

- Notices
- Requests to Know Broadened
- Data Minimization
- Secondary Use Restrictions
- Third Parties
- Security obligations
- Profiling (artificial intelligence) restrictions
- High Risk Assessments

Privacy Notices: Required Revisions

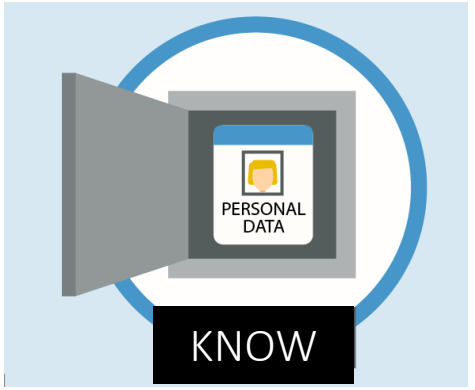
- Notices must **disclose new consumer rights and business responsibilities**, including:



  - Consumer's **Right to Opt Out of Sale of Sharing or Personal Information:**
    - "A business that sells consumers' personal information to, or shares it with, third parties **shall provide notice** to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold or shared and that consumers have the 'right to opt-out' of the sale or sharing of their personal information." 1798.120(b).
  - Consumers' **Right to Limit Use and Disclosure of Sensitive Personal Information**:
    - "A business that uses or discloses a consumer's sensitive personal information for purposes other than those specified in this subdivision **shall provide notice** to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be used, or disclosed to a service provider or contractor, for additional, specified purposes and that consumers have the right to limit the use or disclosure of their sensitive personal information." 1798.121(b).

Requests to Know Broadened

- **Expanded to be consistent with "sharing"** concept, *e.g.:*
  - "A consumer shall have the right to request that a business that sells or shares the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer . . . . " 1798.115(a).
- Potentially **expands time period**:
  - "The disclosure of the required information shall cover the 12-month period preceding the business's receipt of the verifiable consumer request, provided that . . . A consumer may request that the business disclose the required information beyond the 12-month period and the business shall be required to provide such information unless doing so proves impossible or would involve a disproportionate effort." 1798.130(a)(2)(B).
- **Clarifies the "specific pieces of personal information" requirement:**
  - "Provide the specific pieces of personal information obtained from the **consumer in a format that is easily understandable to the average consumer**, and to the extent technically feasible, in **a structured, commonly used, machine-readable format** that may also be transmitted to another entity at the consumer's request without hindrance. 'Specific pieces of information' **do not include data generated to help ensure security and integrity** or as prescribed by regulation." 1798.130(a)(3)(B)(iii).



Data Minimization & Retention

- Businesses must **inform consumers of the length of time** the business intends to retain each category of PI, including Sensitive PI:
  - If it is not possible, the business must provide the criteria used to determine the retention period
- Businesses **cannot retain the consumer's PI or Sensitive PI longer than is "reasonable necessary"**:
  - "The **length of time the business intends to retain** each category of personal information, including sensitive personal information, or **if that is not possible, the criteria used** to determine that period provided that a business **shall not retain** a consumer's personal information or sensitive personal information for each disclosed purpose for which the personal information was collected **for longer than is reasonably necessary** for that disclosed purpose." 1798.100(a)(3).

Secondary Use Restrictions

- PI **use must be "reasonably necessary" and "proportionate"** with the **purpose of collection**:
  - "A business' collection, use, retention, and sharing of a consumer's personal information shall be **reasonably necessary and proportionate** to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and **not further processed in a manner that is incompatible with those purposes**." 1798.100(c).
- **Same for Sensitive PI**:
  - "A business **shall not** collect additional categories of sensitive personal information or **use sensitive personal information collected for additional purposes** that are **incompatible with the disclosed purpose** for which the sensitive personal information was collected without providing the consumer with notice consistent with this section." 1798.100(a)(2).

Third Parties: Requirements

- Businesses must **enter into agreements with third parties** to carry out CPRA obligations:
  - "A business that collects a consumer's personal information and that **sells** that personal information to, or **shares** it with, a third party or that **discloses** it to a **service provider** or **contractor** for a business purpose shall enter into an agreement with the third party, service provider, or contractor . . . ." 1798.100(d).
- Businesses **must relay deletion requests to third parties**, if they have received the information, unless impossible:
  - "A business that receives a verifiable consumer request from a consumer to delete the consumer's personal information . . . shall delete the consumer's personal information from its records, ~~and direct~~ **notify** any service providers or contractors to delete the consumer's personal information from their records, and **notify all third parties to whom the business has sold or shared the personal information to delete** the consumer's personal information **unless this proves impossible or involves disproportionate effort**." 1798.105(c)(1).
- And those third parties must also extend that notification, as necessary. 1798.105(c)(3).

Certain Security Obligations Clarified

- CPRA clarifies security obligations by **creating an affirmative obligation** to provide **"reasonable" security measures**:
  - A business that collects a consumer's personal information shall implement **reasonable security procedures and practices appropriate to the nature of the personal information** to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Section 1798.81.5." 1798.100(e).

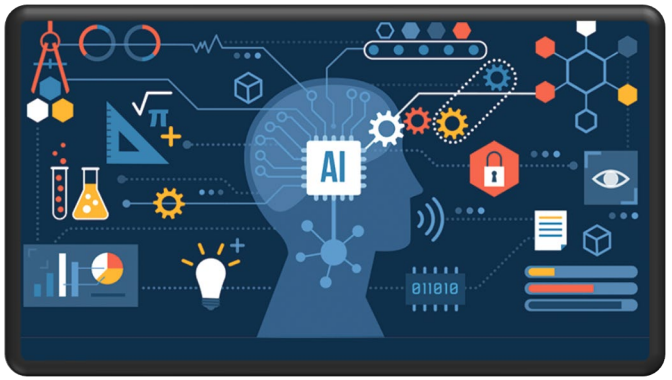
- CPRA service provider agreements should obligate the service provider to comply with applicable obligations under the title and offer the same level of protection.
- Encrypted and redacted information (sufficient to fall outside of limited private right of action) remains undefined.
- "Deidentified" redefined consistent with FTC 3-part test.

High Risk Assessments

- CPRA calls for regulations relating to **processing that poses a "significant risk" to consumers' privacy or security**:
  - Such businesses will be required to **perform internal assessments** and **submit risk assessment to the California Privacy Protection Agency** on a "**regular basis**," including:
    - **"…whether the processing involves sensitive personal information, and identifying and weighing the benefits resulting from the processing to the business, the consumer**, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing, with the goal of restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits . . . ."
- Factors to be considered when determining whether processing presents "significant risk" include "size" and "complexity of business and nature/scope of processing activities. 1798.185(a)(15).

AI: "Profiling" Restriction

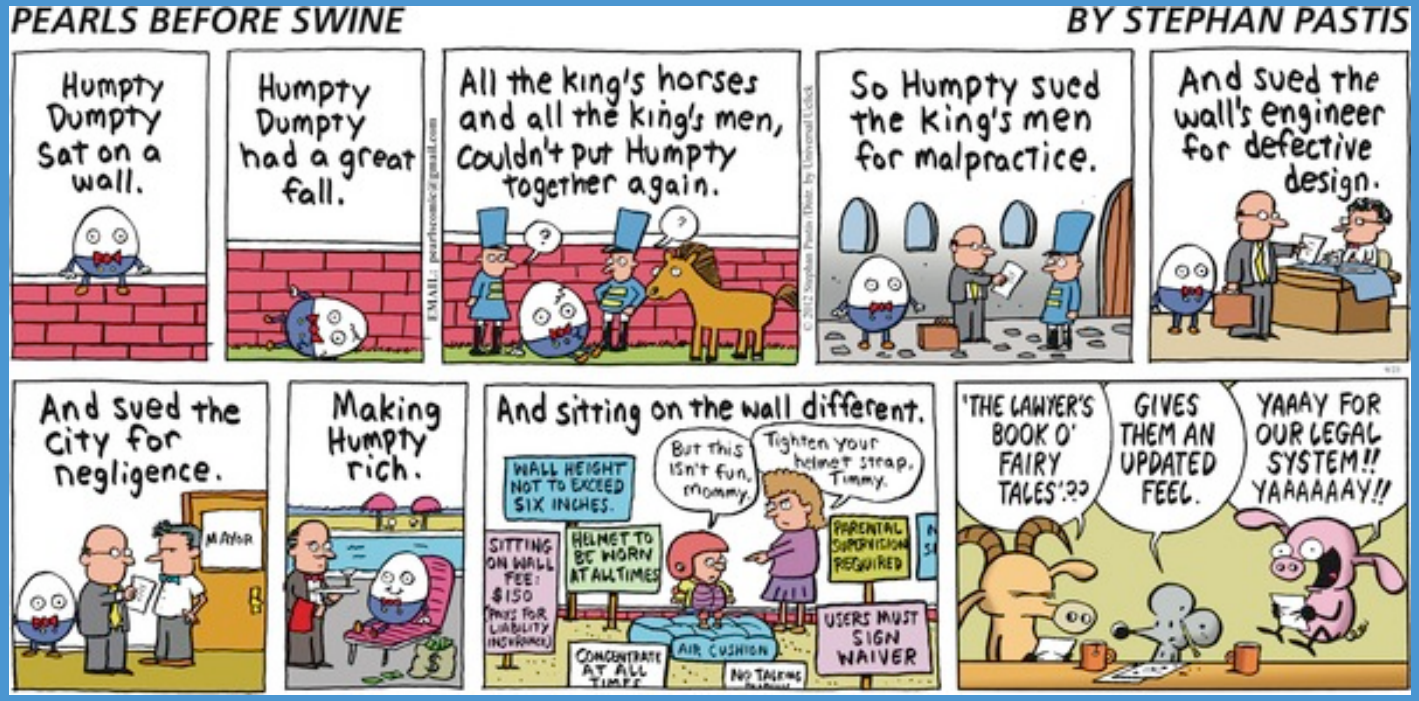
- Intended to address **automated systems or artificial intelligence** that may result in discrimination:
  - "'Profiling' means any form of **automated processing of personal information**, as further defined by regulations pursuant to paragraph (16) of subdivision (a) of Section 1798.185, to **evaluate** certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's **performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements**." 1798.140(z).
- AG and then California Privacy Protection Agency required to **adopt regulations** "governing access and opt-out rights with respect to a business's use of automated decision-making technology, including profiling…"



What Remains Unclear

- Many topics are designated to be fleshed out by future regulations:
  - Audits and risk assessments for procession that poses a "significant risk to consumers' privacy or security"
  - Interaction of CPRA with employees
  - Operation of right to correct
  - Definition for "business purposes"
  - Automated decision rules ("profiling")
  - Service provider rules
  - Right to know rules
  - Operation of opt-out signals

GIBSON DUNN



Class Actions & AG Enforcement to Date

Key Cases From Last Year

- *Burke v. Clearview AI, Inc.* (S.D.N.Y. No. 1:20-cv-03104):
  - Plaintiffs allege that "Clearview illicitly 'scraped' hundreds, if not thousands or more, websites, such as Facebook, Twitter, and Google, for over three billion images of consumers' faces."
  - Plaintiffs do not allege a CCPA claim directly based on allegations of collection and use without disclosure. Instead, they attempt to bootstrap it to a UCL claim.
  - Transferred to MDL in the Northern District of Illinois (MDL No.
- *Cullen v. Zoom Video Commc'ns Inc.* (N.D. Cal. No. 5:20-cv-02155-SVK) and Similar Cases:
  - *Hurvitz v. Zoom, Facebook, & LinkedIn* (C.D. Cal. No. 2:20-cv-03400); *Taylor* (N.D. Cal. No. 5:20-cv-02170); *Johnston* (N.D. Cal. No. 5:20-cv-02376); *Kondrat* (N.D. Cal. No. 5:20-cv-02520); *Lawton* (N.D. Cal. No. 5:20-cv-02592); *Jimenez*, (N.D. Cal. No. 5:20-cv-02591); *Hartmann* (N.D. Cal. No. 5:20-cv-02620); *Henry* (N.D. Cal. No. 5:20-cv-02691).
  - These putative class actions generally allege that Zoom wrongfully shared sensitive information with Facebook. Some also allege a lack of adequate encryption (still undefined under CPRA).
  - Some bring claims directly under the CCPA; others bootstrap to the UCL.

Key Cases From Last Year

- *Barnes v. Hanna Andersson & Salesforce* (N.D. Cal. No. 3:20-cv-00812-DMR):
  - The plaintiff alleges that "[h]ackers not only 'scraped' many of Hanna's customers' names from the website [hosted by Salesforce] by infecting it with malware, they also stole customers' billing and shipping addresses, payment card numbers, CVV codes, and credit card expiration dates."
  - The complaint alleges violations of the UCL and the CCPA's data breach provision, § 1798.150, which provides for a private right of action for "unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information."
  - The complaint also brings a negligence claim.
  - Retroactive? Can a plaintiff bring a CCPA claim based on events that predate the law going into effect on January 1?
  - Settlement fund of $400,000. Plaintiffs' counsel can seek up to $100,000 for fees.

GIBSON DUNN

Our Privacy, Cybersecurity & Consumer Protection Practice

Privacy, Cybersecurity and Consumer Protection Practice

Gibson Dunn represents many leading companies in their most important privacy and data security matters, and regularly is called upon to handle among the most challenging controversies and transactions that arise in this area, ranging from high-stakes M&A, to significant FTC actions and other regulatory investigations, enforcement actions by EU data protection authorities, and complex consumer class action litigation and criminal matters.

The firm's Privacy, Cybersecurity and Consumer Protection practice brings together a team of attorneys with extensive experience both in private practice and at senior government levels. We have the deepest bench of former cyber-crime prosecutors of any firm and we deploy that expertise, along with a wide range of other experts around the globe and former senior US and foreign government officials, to guide clients through their most challenging issues. Our practice also stands out for the remarkable breadth of privacy and data security issues we handle, as well as their high-profile nature. And our lawyers are distinguished not only by their substantive capabilities and advocacy skills, but also by their ability to guide clients through major events, deal with all relevant constituencies, and develop and implement a prompt and effective crisis management strategy.

Chambers USA 2020 recognized Gibson Dunn for Privacy & Data Security nationwide and ranked Alexander Southwell individually, highlighting the firm's "highly regarded privacy and cybersecurity offering."

Noting that Gibson Dunn is "the trusted choice for leading technology companies" and "continues to do some of the most cutting-edge work in the space," *Law360* named the firm a 2017, 2018 and 2019 Cybersecurity & Privacy Practice Group of the Year.

Gibson Dunn was named to BTI Consulting Group's 2020 Leading Law Firms in Cybersecurity & Data Privacy list. The firm was also named.one of the seven Law Firms Best at Cybersecurity in BTI's 2017 report based on in-depth interviews with more than 320 corporate counsel at the world's largest companies.

Privacy, Cybersecurity and Consumer Protection Practice

Our Privacy, Cybersecurity and Consumer Protection Practice Group represents clients across a wide range of industries in high stakes matters involving complex and rapidly evolving laws, regulations, and industry best practices relating to privacy, cybersecurity, and consumer protection.

- Privacy. We have decades of experience with a wide array of privacy counseling, government investigations, and litigation. Our deep roster of attorneys with experience at the highest levels of government is prepared to handle any type of government investigation. Our elite class action team has successfully litigated many cutting-edge cases, including numerous matters of first impression. Our experience includes advising a broad array of companies large and small, in Silicon Valley, Silicon Alley, and around the world.
- Cybersecurity. We have substantial experience assisting companies with all facets of cybersecurity, including counseling clients through the important steps that must occur immediately after breach situations and navigating the federal and state government investigations, media attention, and private litigation that increasingly accompany cybersecurity incidents.
- Consumer Protection. We advise clients on a broad array of consumer protection issues, including privacy and data security, advertising practices, consumer disclosures, and compliance with the myriad laws regulating consumer interactions. We routinely appear before the U.S. Federal Trade Commission, the U.S. Department of Justice, and state Attorneys General on consumer protection matters and have litigated complex consumer protection disputes involving a diverse range of industries.

Our attorneys have extensive experience conducting privacy and information security due diligence in support of mergers and acquisitions and other corporate transactions and advise on all aspects of technology, data and privacy-related corporate transactions. We also assist with counseling on securities law disclosures, and regularly advise boards of directors and in-house counsel on governance matters, privacy and cybersecurity policies and procedures, risk management frameworks, incident response plans, and best practices related to preparedness.

Privacy, Cybersecurity and Consumer Protection Practice Leaders

Alexander H. Southwell
NY | Partner and Co-Chair
Privacy, Cybersecurity and Consumer Protection

Nationally recognized thought leader on data privacy and cybersecurity, Alex served as an Assistant U.S. Attorney with primary responsibility for investigating and prosecuting computer crime cases. He is regularly called upon by a wide-range of leading global companies to counsel on — as well as handle investigations, enforcement defense, and litigation related to — an array of privacy, information technology, data breach, theft of trade secrets and intellectual property, computer fraud, and network and data security issues.

Ranked by *Chambers USA* 2020 in Privacy & Data Security: Litigation. Sources note that Alex "has a keen eye for attention to detail, client service and navigating a complex legal and regulatory landscape."

Cybersecurity Docket's 2018 Incident Response 30, honoring the "30 best and brightest data breach response lawyers."

Law360 "MVP" in Privacy in both 2015 and 2016 – one of five "elite attorneys" who have "distinguished themselves from their peers by securing hard-earned successes in high-stakes litigation, complex global matters and record-breaking deals."

The National Law Journal's 2015 Cybersecurity & Data Privacy Trailblazers for the successful representation of a prominent executive search firm facing a serious cyberattack and mitigating the fallout of the crisis.

Ahmed Baladi
Paris | Partner and Co-Chair
Privacy, Cybersecurity and Consumer Protection

With renowned experience in a wide range of privacy and cybersecurity matters including compliance and governance programs in light of the GDPR, Ahmed regularly represents companies and corporate executives on investigations and procedures before the French data protection authority and other national DPAs as well as administrative courts. He also advises a variety of clients on data breach and national security matters including handling investigations, enforcement defense and crisis management.

2019 Lawyer of the Year:
Paris Information and Technology Law by *The Best Lawyers*™ in France 2019.

Chambers Europe 2020 :
TMT: Information Technology and Data Protection spotlight Table (France). Sources note that Ahmed is "very smart and bright." - "He is patient and always tries to find intelligent compromises."

The Legal 500 EMEA 2019
in the France: Industry Focus:
IT, telecoms and the internet category, and as a "Leading Individual"

Our Offices

Beijing
Unit 1301, Tower 1
China Central Place
No. 81 Jianguo Road
Chaoyang District
Beijing 100025, P.R.C.
+86 10 6502 8500

Brussels
Avenue Louise 480
1050 Brussels
Belgium
+32 (0)2 554 70 00

Century City
2029 Century Park East
Los Angeles, CA 90067-3026
+1 310.552.8500

Dallas
2001 Ross Avenue, Suite 2100
Dallas, TX 75201
+1 214.698.3100

Denver
1801 California Street
Denver, CO 80202-2642
+1 303.298.5700

Dubai
Building 5, Level 4
Dubai International Finance Centre
P.O. Box 506654
Dubai, United Arab Emirates
+971 (0)4 318 4600

Frankfurt
TaunusTurm
Taunustor 1
60310 Frankfurt
Germany
+49 69 247 411 500

Hong Kong
32/F Gloucester Tower, The Landmark
15 Queen's Road Central
Hong Kong
+852 2214 3700

Houston
811 Main Street, Suite 3000
Houston, TX 77002
+1 346.718.6600

London
Telephone House
2-4 Temple Avenue
London EC4Y 0HB
England
+44 (0) 20 7071 4000

Los Angeles
333 South Grand Avenue
Los Angeles, CA 90071-3197
+1 213.229.7000

Munich
Hofgarten Palais
Marstallstrasse 11
80539 Munich
Germany
+49 89 189 33-0

New York
200 Park Avenue
New York, NY 10166-0193
+1 212.351.4000

Orange County
3161 Michelson Drive
Irvine, CA 92612-4412
+1 949.451.3800

Palo Alto
1881 Page Mill Road
Palo Alto, CA 94304-1125
+1 650.849.5300

Paris
16, avenue Matignon
75008 Paris
France
+33 (0)1 56 43 13 00

San Francisco
555 Mission Street
San Francisco, CA 94105-0921
+1 415.393.8200

São Paulo
Rua Funchal, 418, 35°andar
Sao Paulo 04551-060
Brazil
+55 (11)3521.7160

Singapore
One Raffles Quay
Level #37-01, North Tower
Singapore 048583
+65.6507.3600

Washington, D.C.
1050 Connecticut Avenue, N.W.
Washington, D.C. 20036-5306
+1 202.955.8500