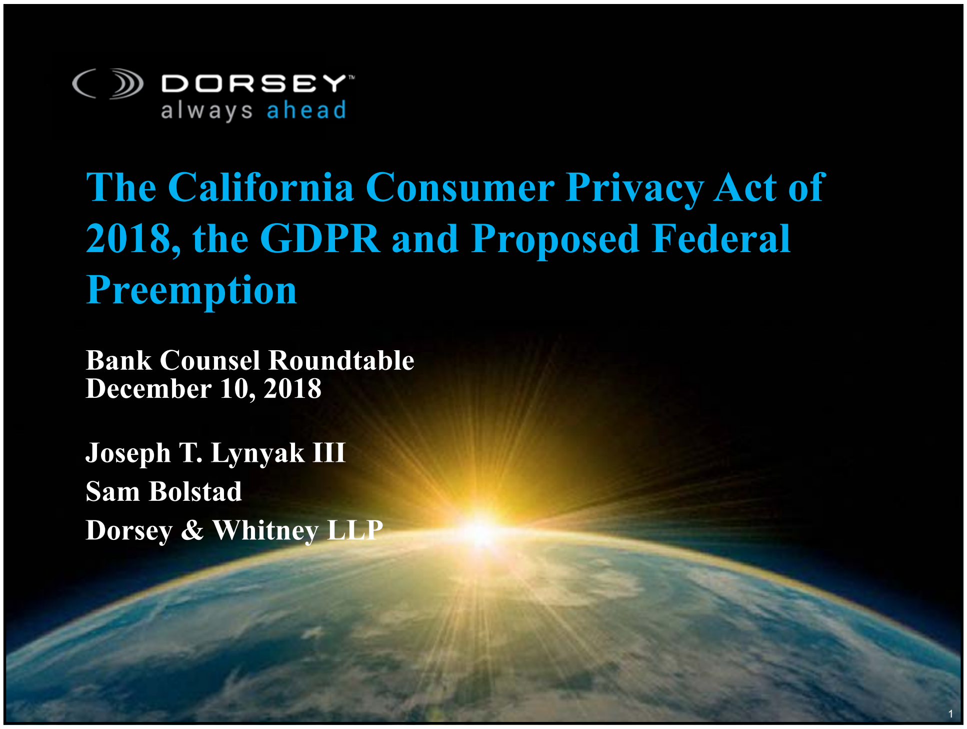
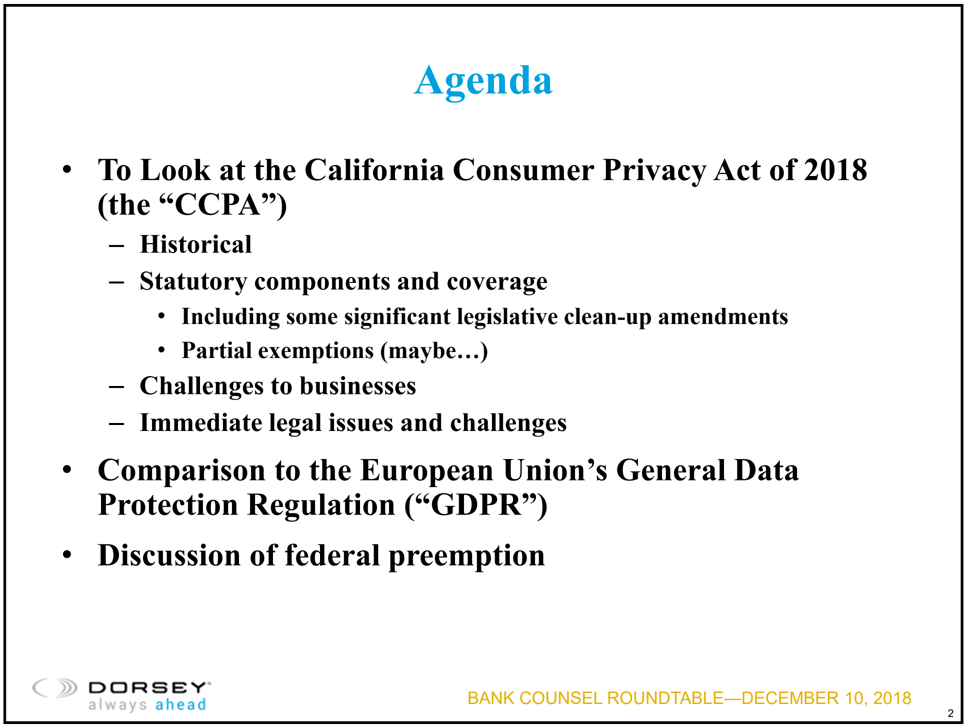


The California Consumer Privacy Act of 2018, the GDPR and Proposed Federal Preemption

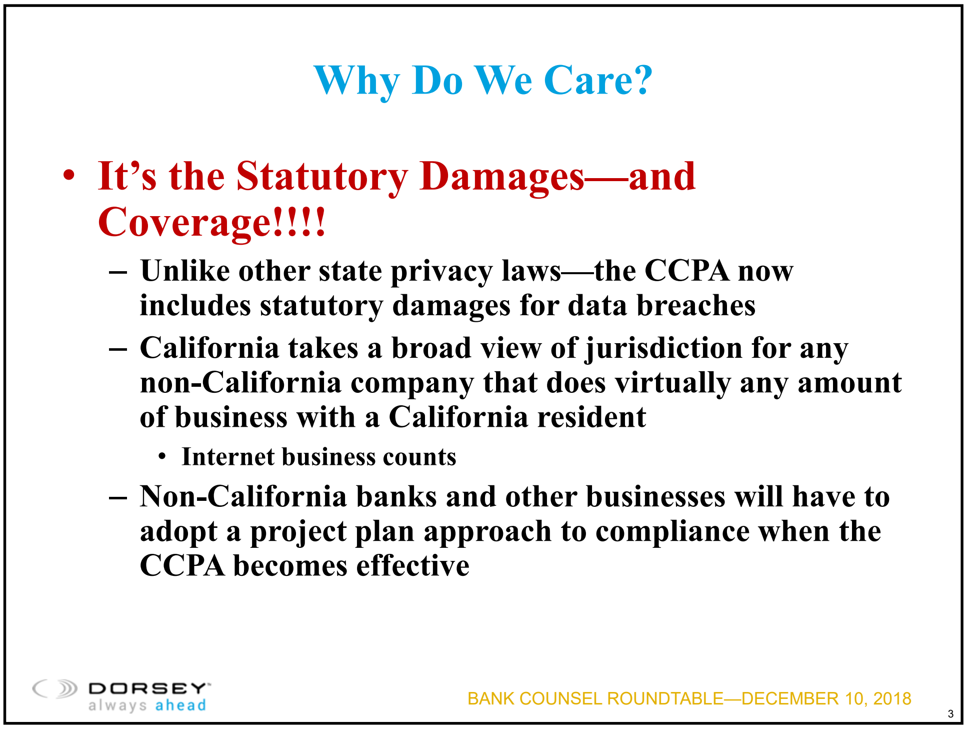
Bank Counsel Roundtable
December 10, 2018

Joseph T. Lynyak III
Sam Bolstad
Dorsey & Whitney LLP



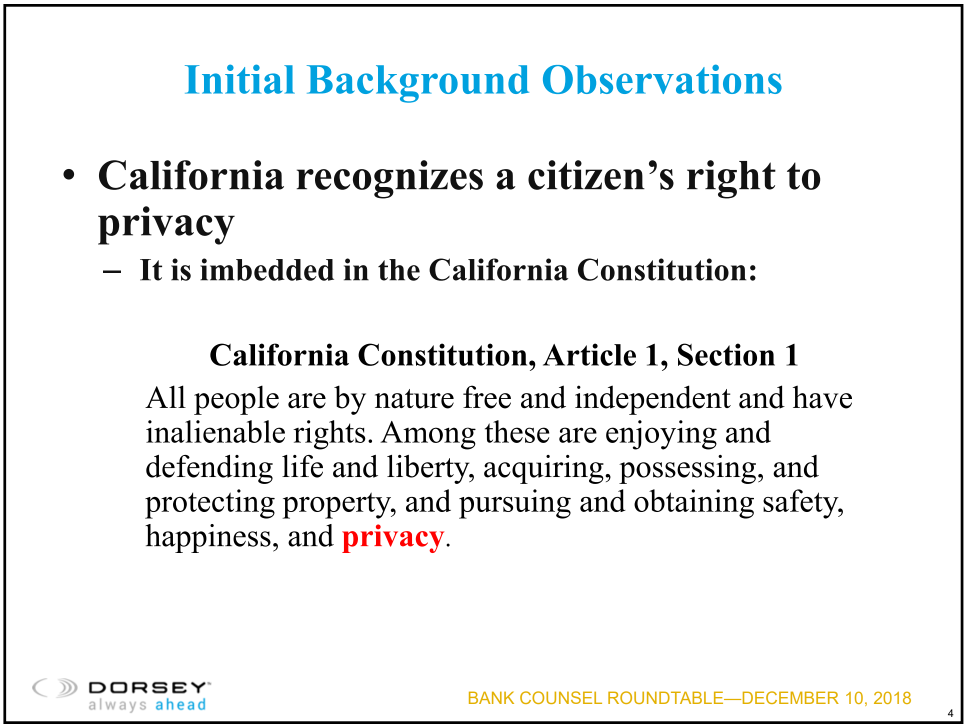
Agenda

- To Look at the California Consumer Privacy Act of 2018 (the "CCPA")
  - Historical
  - Statutory components and coverage
    - Including some significant legislative clean-up amendments
    - Partial exemptions (maybe…)
  - Challenges to businesses
  - Immediate legal issues and challenges
- Comparison to the European Union's General Data Protection Regulation ("GDPR")
- Discussion of federal preemption



Why Do We Care?

- **It’s the Statutory Damages—and Coverage!!!!**
  - Unlike other state privacy laws—the CCPA now includes statutory damages for data breaches
  - California takes a broad view of jurisdiction for any non-California company that does virtually any amount of business with a California resident
    - Internet business counts
  - Non-California banks and other businesses will have to adopt a project plan approach to compliance when the CCPA becomes effective

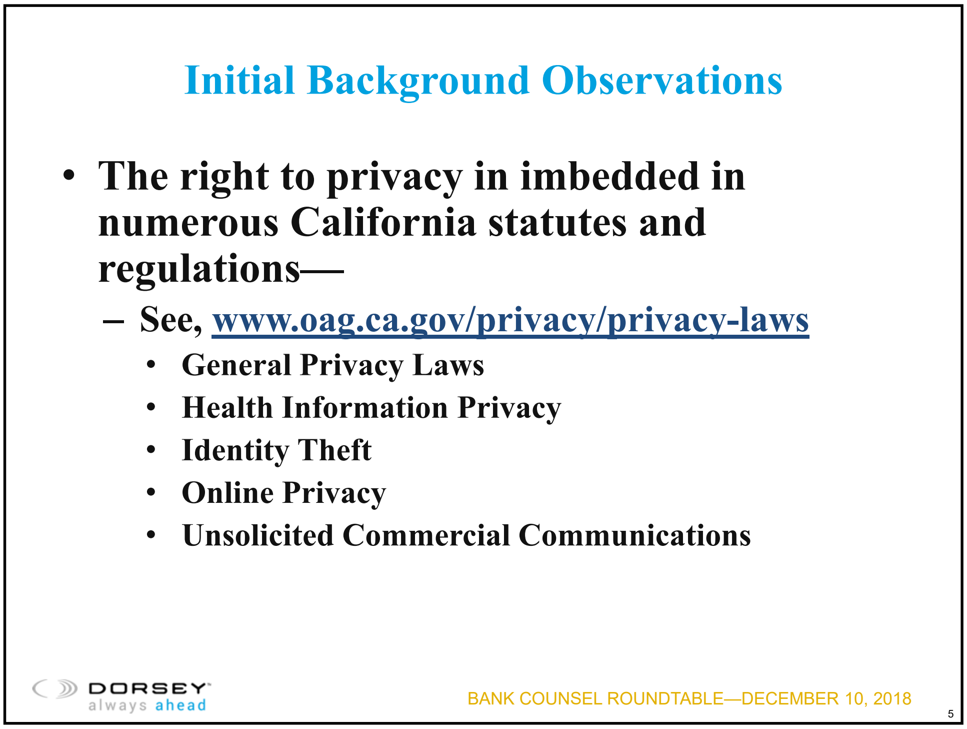


Initial Background Observations

- **California recognizes a citizen’s right to privacy**
  - It is imbedded in the California Constitution:

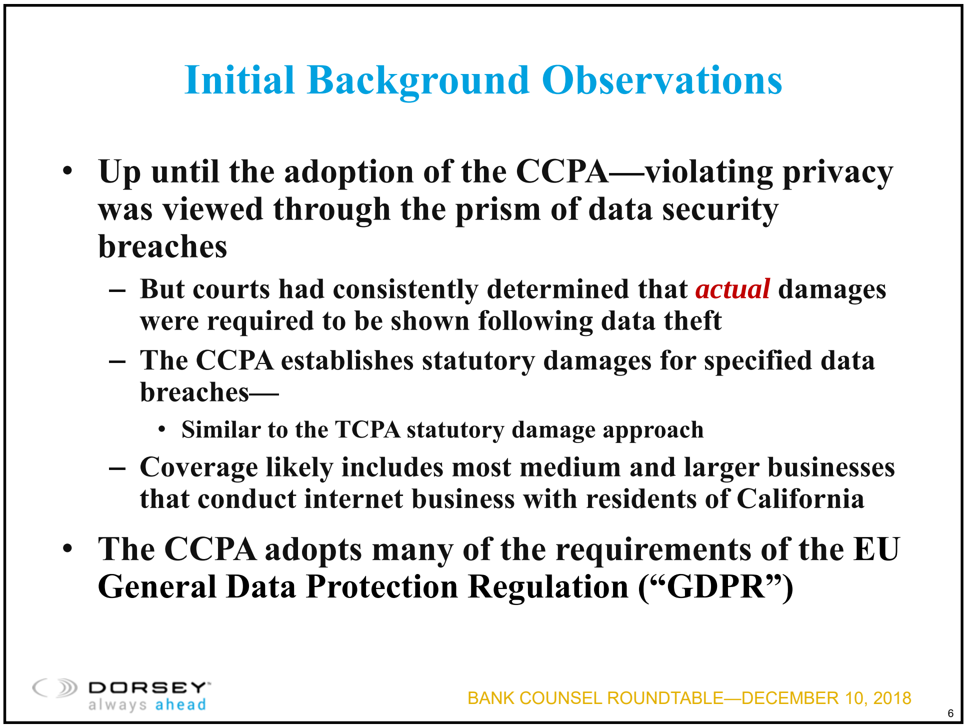
California Constitution, Article 1, Section 1

All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and **privacy**.



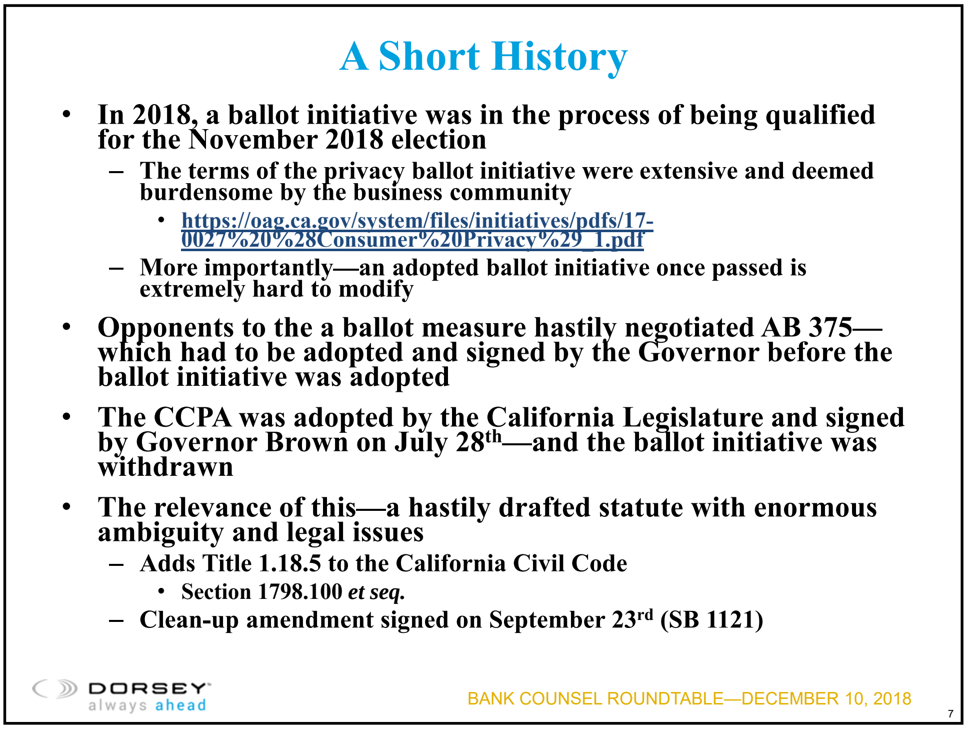
Initial Background Observations

- The right to privacy in imbedded in numerous California statutes and regulations—
  - See, www.oag.ca.gov/privacy/privacy-laws
    - General Privacy Laws
    - Health Information Privacy
    - Identity Theft
    - Online Privacy
    - Unsolicited Commercial Communications



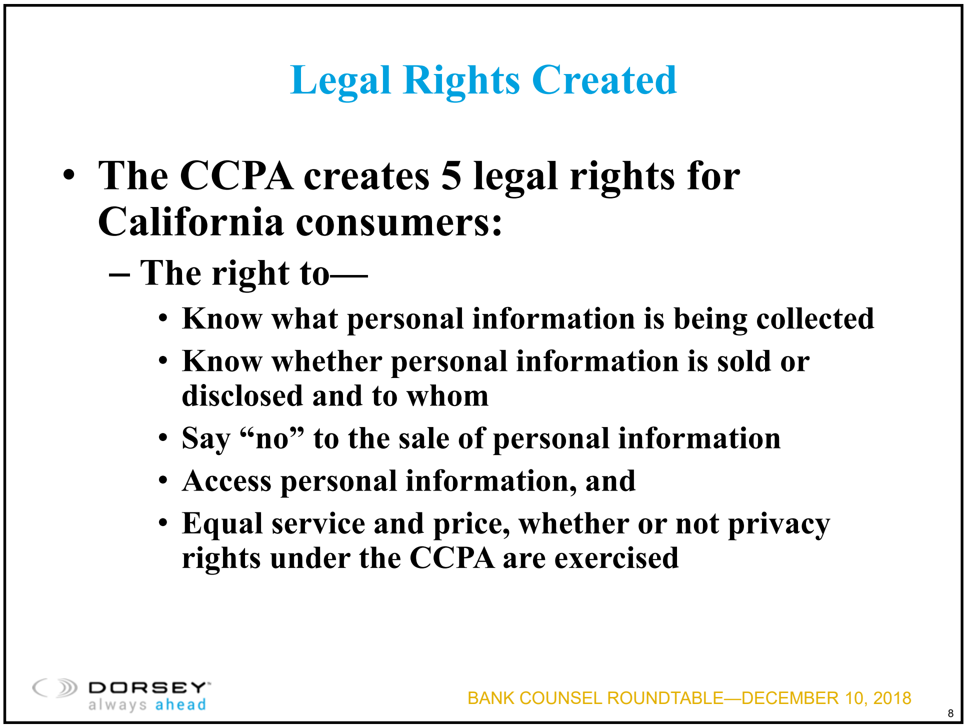
Initial Background Observations

- Up until the adoption of the CCPA—violating privacy was viewed through the prism of data security breaches
  - But courts had consistently determined that *actual* damages were required to be shown following data theft
  - The CCPA establishes statutory damages for specified data breaches—
    - Similar to the TCPA statutory damage approach
  - Coverage likely includes most medium and larger businesses that conduct internet business with residents of California
- The CCPA adopts many of the requirements of the EU General Data Protection Regulation ("GDPR")



A Short History

- In 2018, a ballot initiative was in the process of being qualified for the November 2018 election
  - The terms of the privacy ballot initiative were extensive and deemed burdensome by the business community
    - https://oag.ca.gov/system/files/initiatives/pdfs/17-0027%20%28Consumer%20Privacy%29_1.pdf
  - More importantly—an adopted ballot initiative once passed is extremely hard to modify
- Opponents to the a ballot measure hastily negotiated AB 375—which had to be adopted and signed by the Governor before the ballot initiative was adopted
- The CCPA was adopted by the California Legislature and signed by Governor Brown on July 28th—and the ballot initiative was withdrawn
- The relevance of this—a hastily drafted statute with enormous ambiguity and legal issues
  - Adds Title 1.18.5 to the California Civil Code
    - Section 1798.100 *et seq.*
  - Clean-up amendment signed on September 23rd (SB 1121)



Legal Rights Created

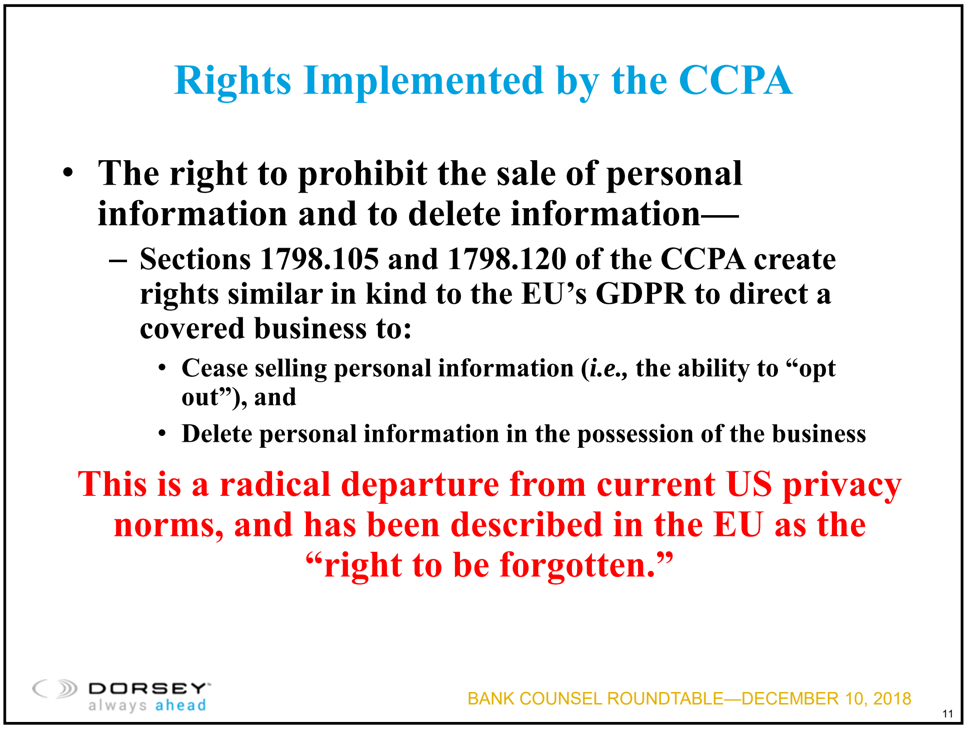
- The CCPA creates 5 legal rights for California consumers:
  - The right to—
    - Know what personal information is being collected
    - Know whether personal information is sold or disclosed and to whom
    - Say “no” to the sale of personal information
    - Access personal information, and
    - Equal service and price, whether or not privacy rights under the CCPA are exercised

Rights Implemented by the CCPA

- **The right to know what personal information is being collected—**
  - **Section 1798.100 of the CCPA allows a "consumer" to require a covered "business" to disclose to the consumer the categories of "personal information" that the business—**
    - **Collects**
    - **Maintains**
    - **Sells, or**
    - **Transfers**

Rights Implemented by the CCPA

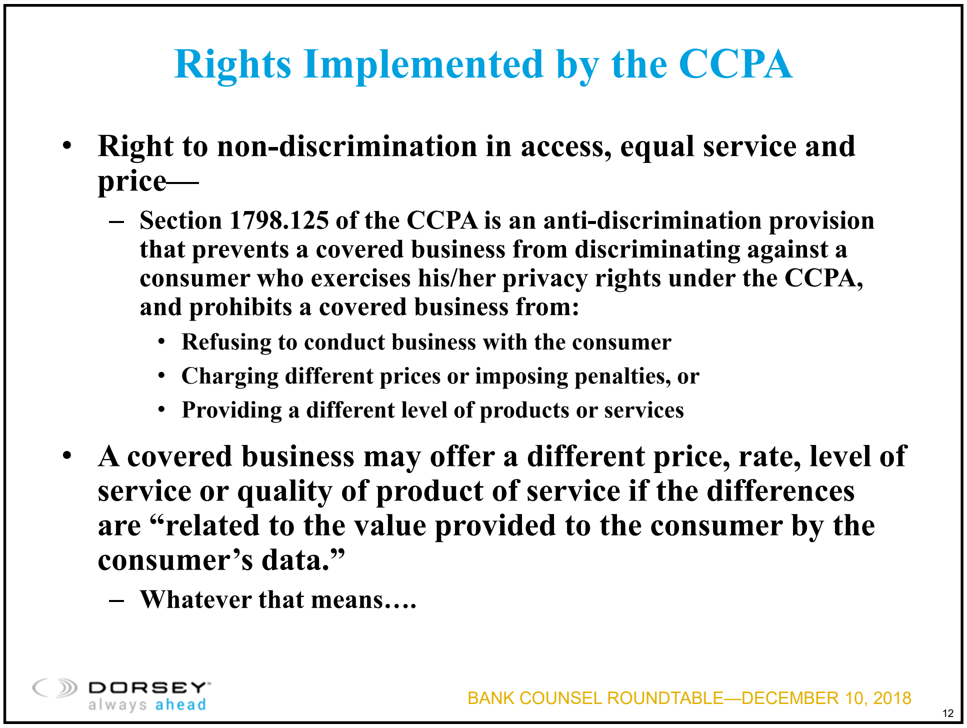
- **The right to know whether personal information is being sold or disclosed and to whom—**
  - **Section 1798.110 of the CCPA requires that, when responding to a "verifiable consumer request," a covered business provide the following:**
    - **The categories of personal information it has collected**
    - **The categories of sources from which the personal information is collected**
    - **The business or commercial purpose for collecting or selling personal information**
    - **The categories of third parties with whom the business shares personal information, and**
    - ***Specific items of personal information the covered business has collected about that consumer***



Rights Implemented by the CCPA

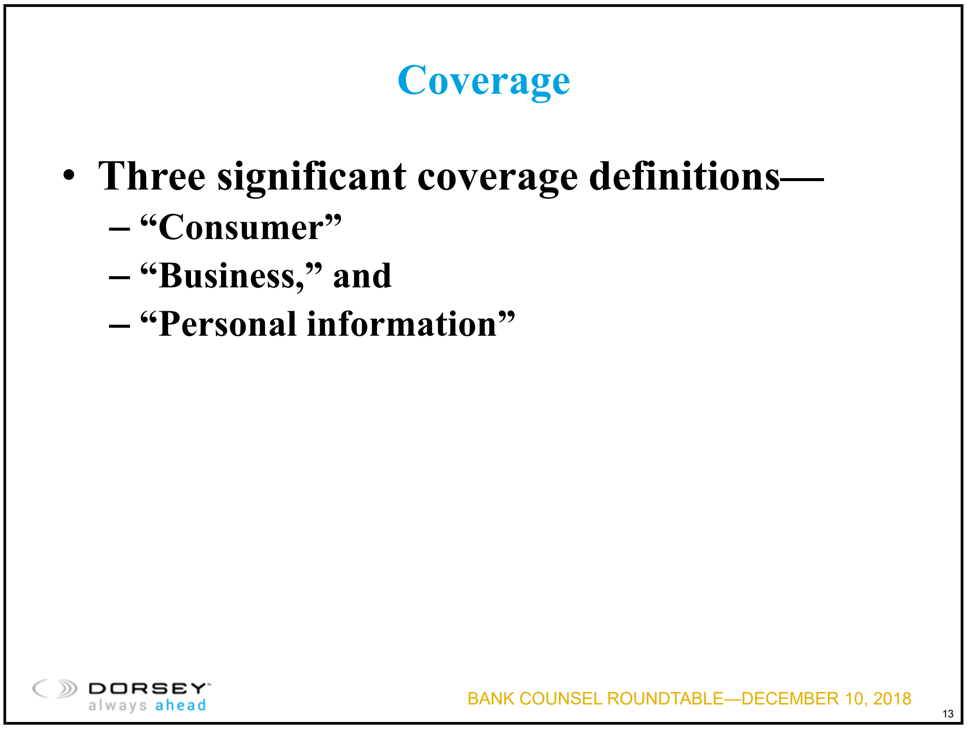
- The right to prohibit the sale of personal information and to delete information—
  - Sections 1798.105 and 1798.120 of the CCPA create rights similar in kind to the EU's GDPR to direct a covered business to:
    - Cease selling personal information (*i.e.*, the ability to "opt out"), and
    - Delete personal information in the possession of the business

This is a radical departure from current US privacy norms, and has been described in the EU as the "right to be forgotten."



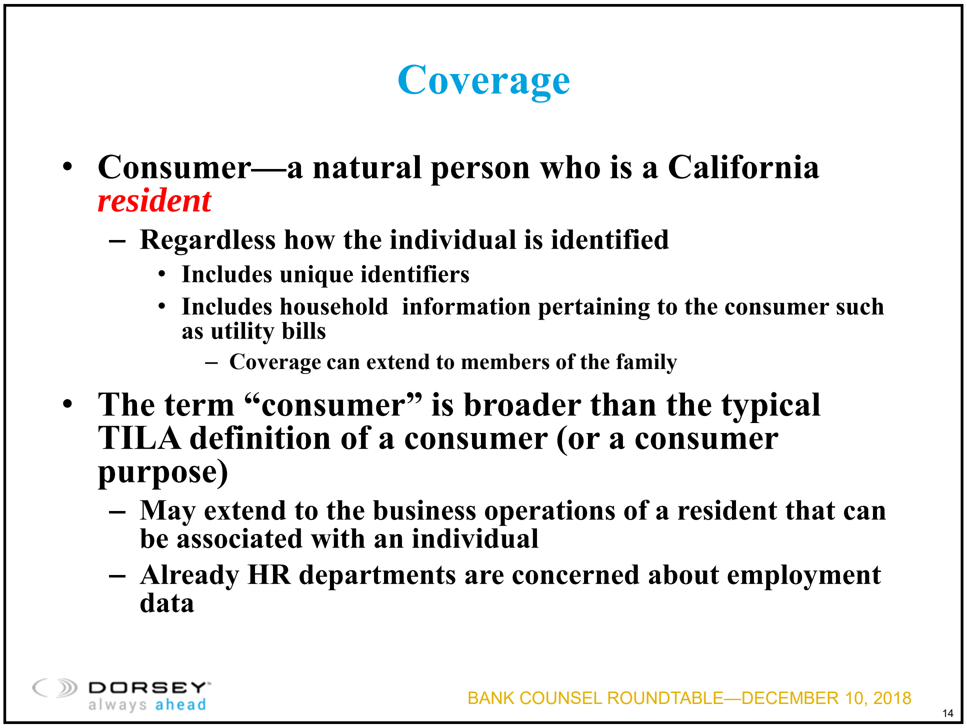
Rights Implemented by the CCPA

- Right to non-discrimination in access, equal service and price—
  - Section 1798.125 of the CCPA is an anti-discrimination provision that prevents a covered business from discriminating against a consumer who exercises his/her privacy rights under the CCPA, and prohibits a covered business from:
    - Refusing to conduct business with the consumer
    - Charging different prices or imposing penalties, or
    - Providing a different level of products or services
- A covered business may offer a different price, rate, level of service or quality of product of service if the differences are "related to the value provided to the consumer by the consumer's data."
  - Whatever that means….



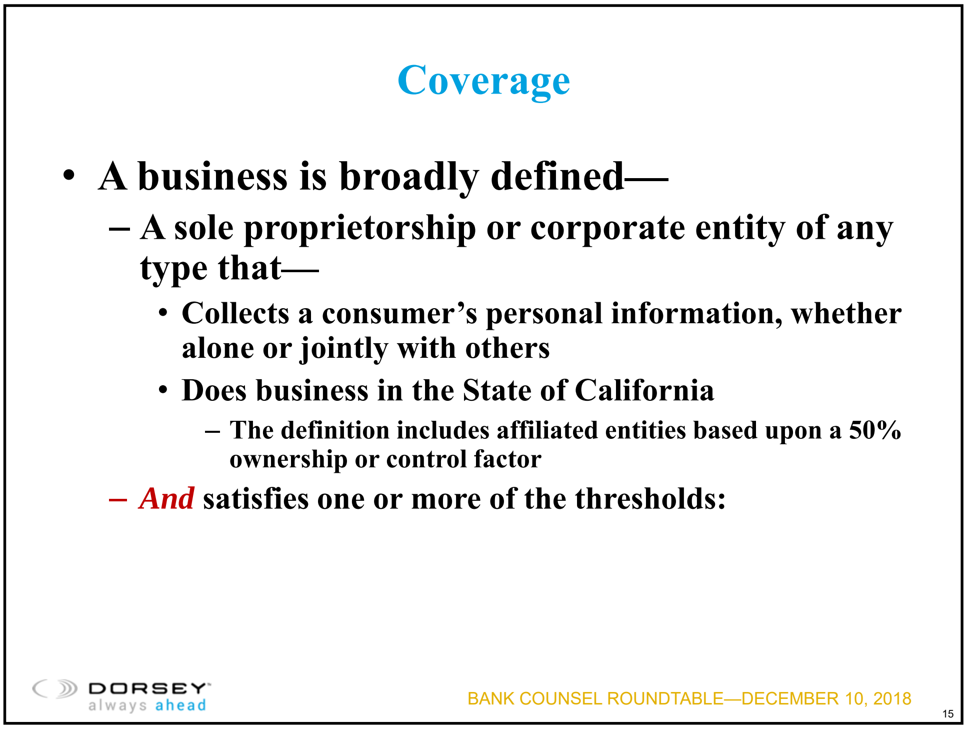
Coverage

- Three significant coverage definitions—
  - “Consumer”
  - “Business,” and
  - “Personal information”



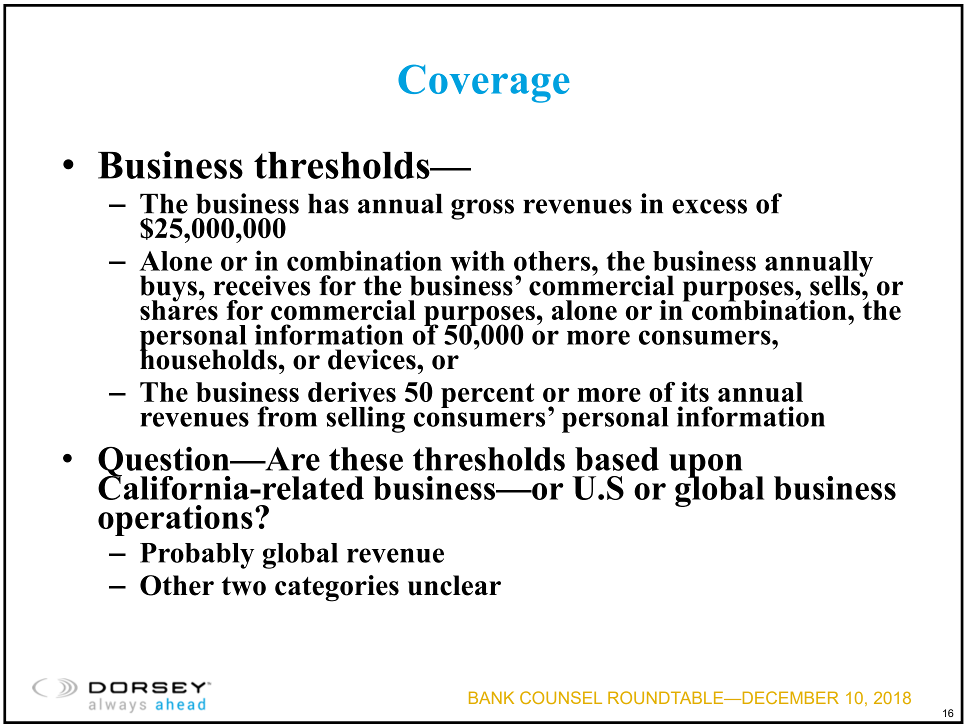
Coverage

- Consumer—a natural person who is a California *resident*
  - Regardless how the individual is identified
    - Includes unique identifiers
    - Includes household information pertaining to the consumer such as utility bills
      - Coverage can extend to members of the family
- The term “consumer” is broader than the typical TILA definition of a consumer (or a consumer purpose)
  - May extend to the business operations of a resident that can be associated with an individual
  - Already HR departments are concerned about employment data



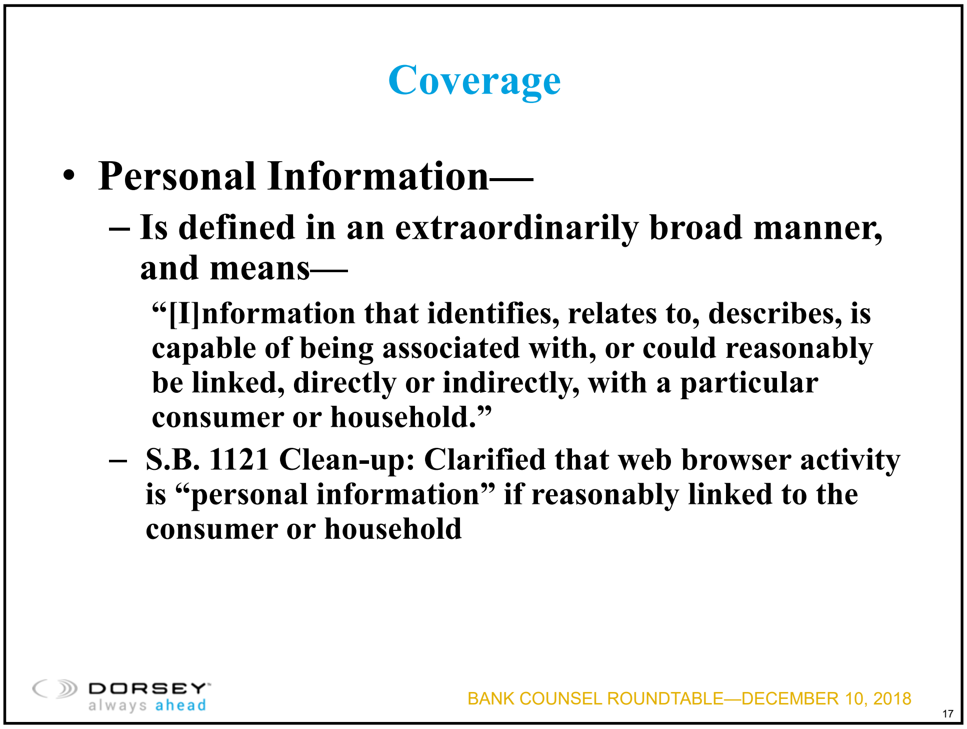
Coverage

- A business is broadly defined—
  - A sole proprietorship or corporate entity of any type that—
    - Collects a consumer's personal information, whether alone or jointly with others
    - Does business in the State of California
      - The definition includes affiliated entities based upon a 50% ownership or control factor
  - *And* satisfies one or more of the thresholds:



Coverage

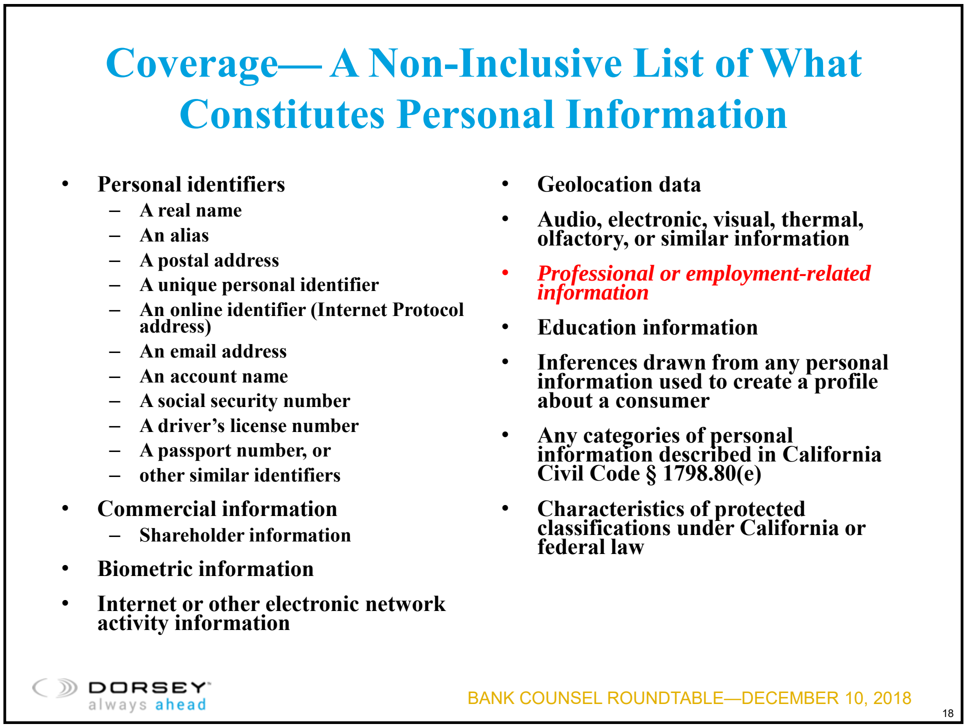
- Business thresholds—
  - The business has annual gross revenues in excess of $25,000,000
  - Alone or in combination with others, the business annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices, or
  - The business derives 50 percent or more of its annual revenues from selling consumers' personal information
- Question—Are these thresholds based upon California-related business—or U.S or global business operations?
  - Probably global revenue
  - Other two categories unclear



Coverage

- **Personal Information—**
  - **Is defined in an extraordinarily broad manner, and means—**

    "[I]nformation 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."
  - **S.B. 1121 Clean-up: Clarified that web browser activity is "personal information" if reasonably linked to the consumer or household**



Coverage— A Non-Inclusive List of What Constitutes Personal Information

- **Personal identifiers**
  - **A real name**
  - **An alias**
  - **A postal address**
  - **A unique personal identifier**
  - **An online identifier (Internet Protocol address)**
  - **An email address**
  - **An account name**
  - **A social security number**
  - **A driver's license number**
  - **A passport number, or**
  - **other similar identifiers**
- **Commercial information**
  - **Shareholder information**
- **Biometric information**
- **Internet or other electronic network activity information**
- **Geolocation data**
- **Audio, electronic, visual, thermal, olfactory, or similar information**
- ***Professional or employment-related information***
- **Education information**
- **Inferences drawn from any personal information used to create a profile about a consumer**
- **Any categories of personal information described in California Civil Code § 1798.80(e)**
- **Characteristics of protected classifications under California or federal law**

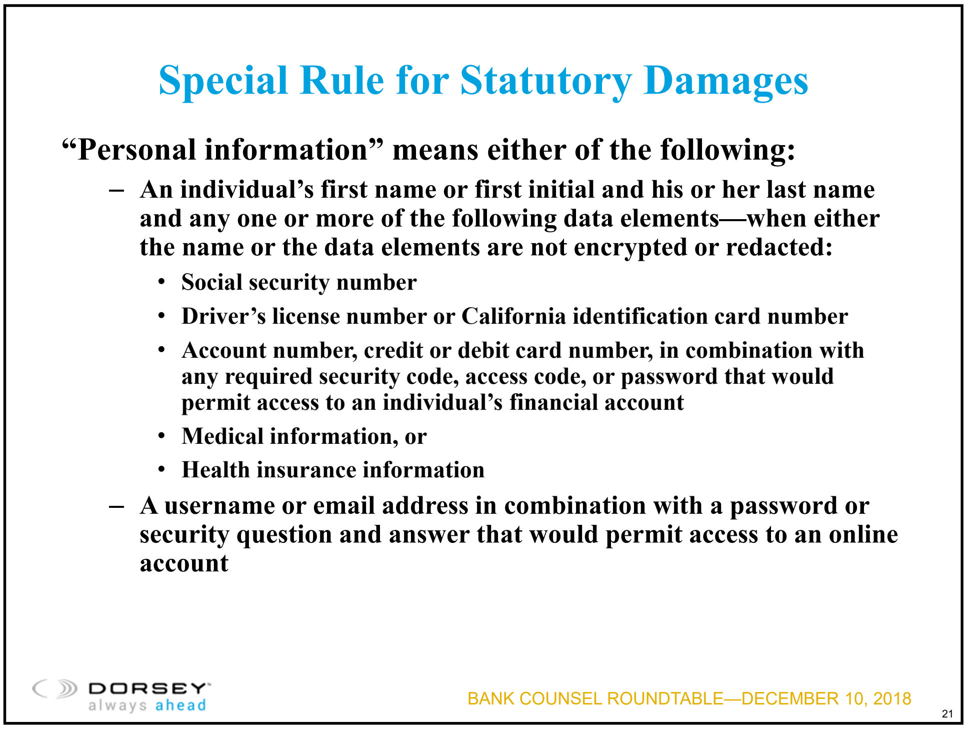
Exceptions

- Several categories of data are exempted, including maintaining data:
  - Used for purposes of completing a transaction with a consumer
  - Sanitized in a manner not useable to identify a consumer (*i.e.,* deidentified data)
  - Used to identify and repair the functionality of a system
  - Used for public or peer reviewed, historical or statistical research
  - Publically available personal information
  - Used to comply with the California Electronic Communications Privacy Act
  - Used to comply with a consumer's data inquiry and instructions
  - Used for security purposes
  - Used for free speech purposes
  - Used to comply with a legal obligation
  - "To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business"
    - Whatever that means…..

Do Waivers Work?

Liability

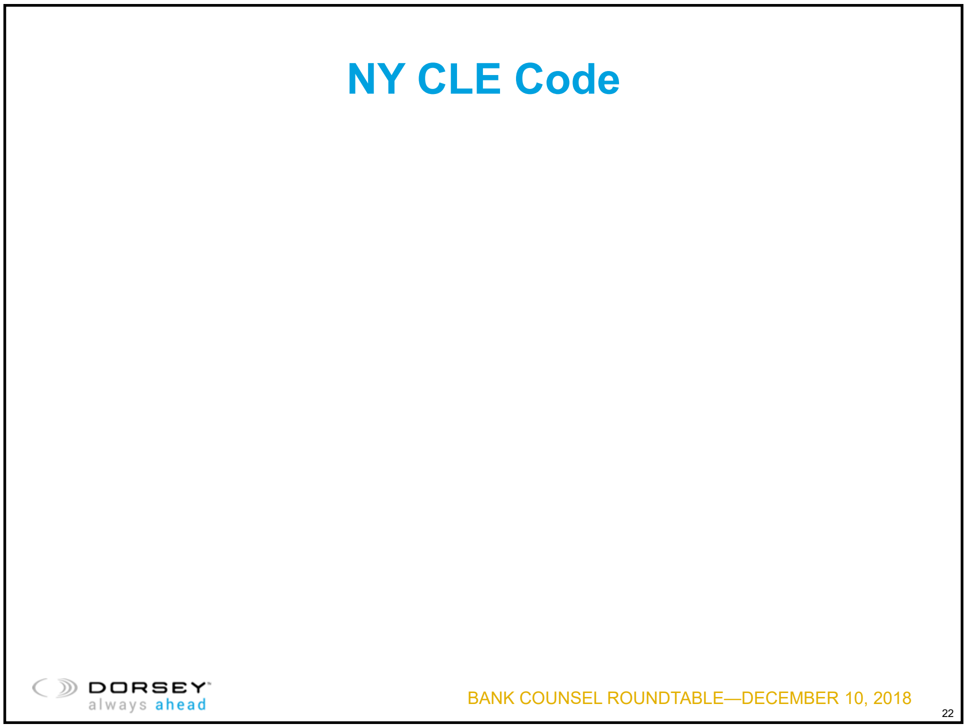
- Actions brought by the Attorney General—
  - $7500 per intentional violation
  - $2500 per unintentional violation
- Actions brought by private parties—
  - Actual damages
  - Statutory damages between $100 and $750 per "incident" for data theft or data security breaches
  - Identification criteria somewhat narrower than general definition of personal information in the CCPA
    - Sole defense appears to be the maintenance of reasonable security protocols
      - How will standards be determined???
- 30-day cure period before AG or private action



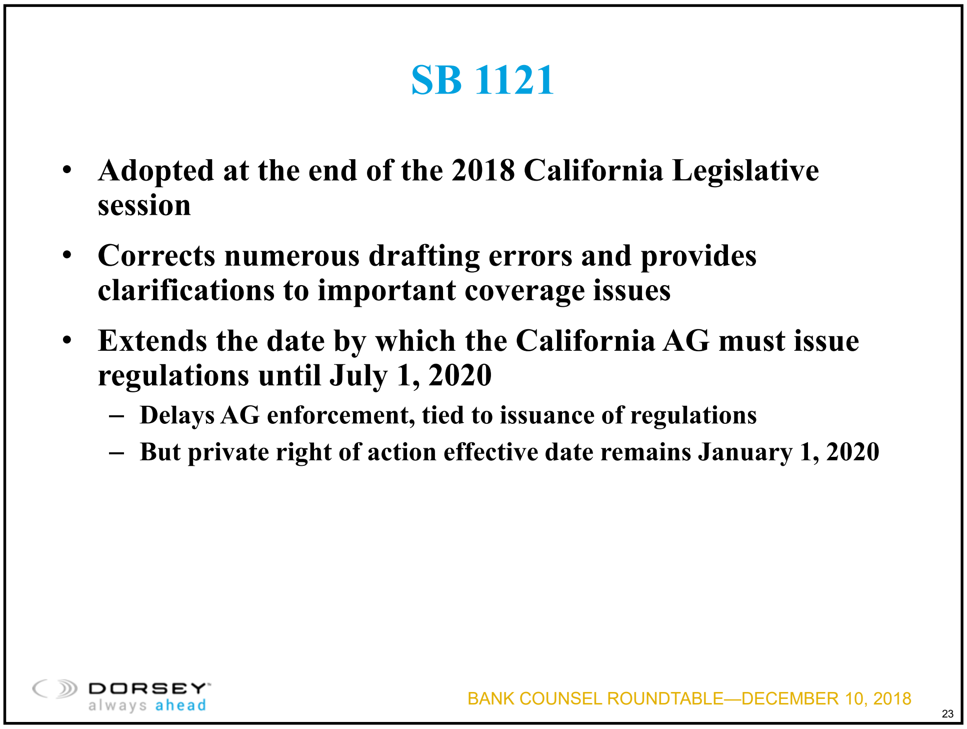
Special Rule for Statutory Damages

"Personal information" means either of the following:

- An individual's first name or first initial and his or her last name and any one or more of the following data elements—when either the name or the data elements are not encrypted or redacted:
  - Social security number
  - Driver's license number or California identification card number
  - Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account
  - Medical information, or
  - Health insurance information
- A username or email address in combination with a password or security question and answer that would permit access to an online account

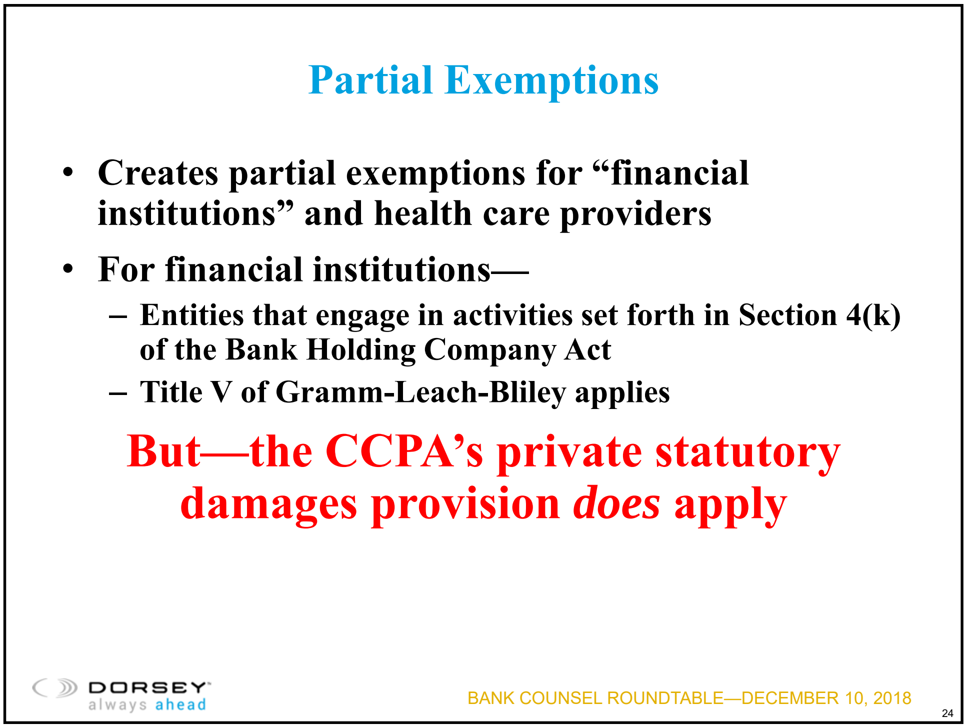


NY CLE Code



SB 1121

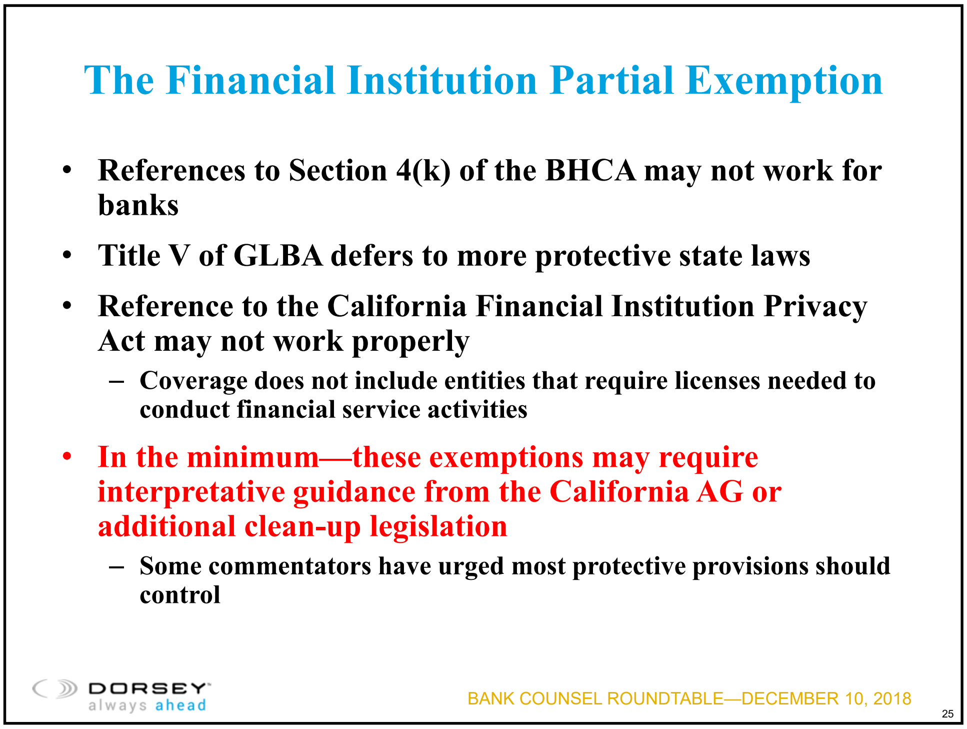
- Adopted at the end of the 2018 California Legislative session
- Corrects numerous drafting errors and provides clarifications to important coverage issues
- Extends the date by which the California AG must issue regulations until July 1, 2020
  - Delays AG enforcement, tied to issuance of regulations
  - But private right of action effective date remains January 1, 2020



Partial Exemptions

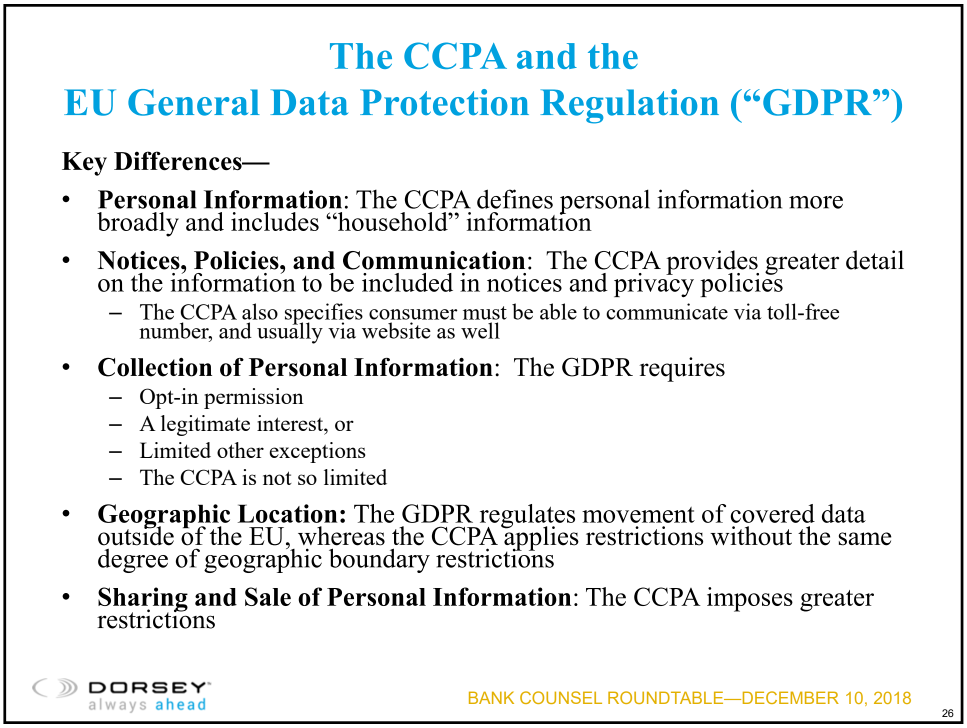
- Creates partial exemptions for "financial institutions" and health care providers
- For financial institutions—
  - Entities that engage in activities set forth in Section 4(k) of the Bank Holding Company Act
  - Title V of Gramm-Leach-Bliley applies

But—the CCPA's private statutory damages provision *does* apply



The Financial Institution Partial Exemption

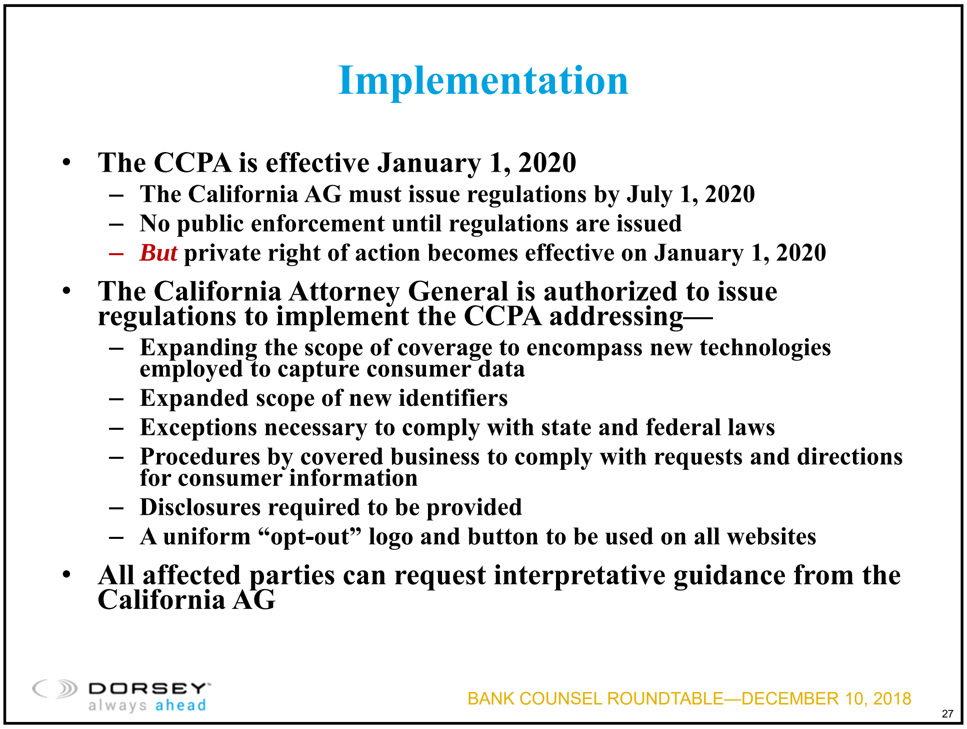
- **References to Section 4(k) of the BHCA may not work for banks**
- **Title V of GLBA defers to more protective state laws**
- **Reference to the California Financial Institution Privacy Act may not work properly**
  - **Coverage does not include entities that require licenses needed to conduct financial service activities**
- **In the minimum—these exemptions may require interpretative guidance from the California AG or additional clean-up legislation**
  - **Some commentators have urged most protective provisions should control**



The CCPA and the EU General Data Protection Regulation (“GDPR”)

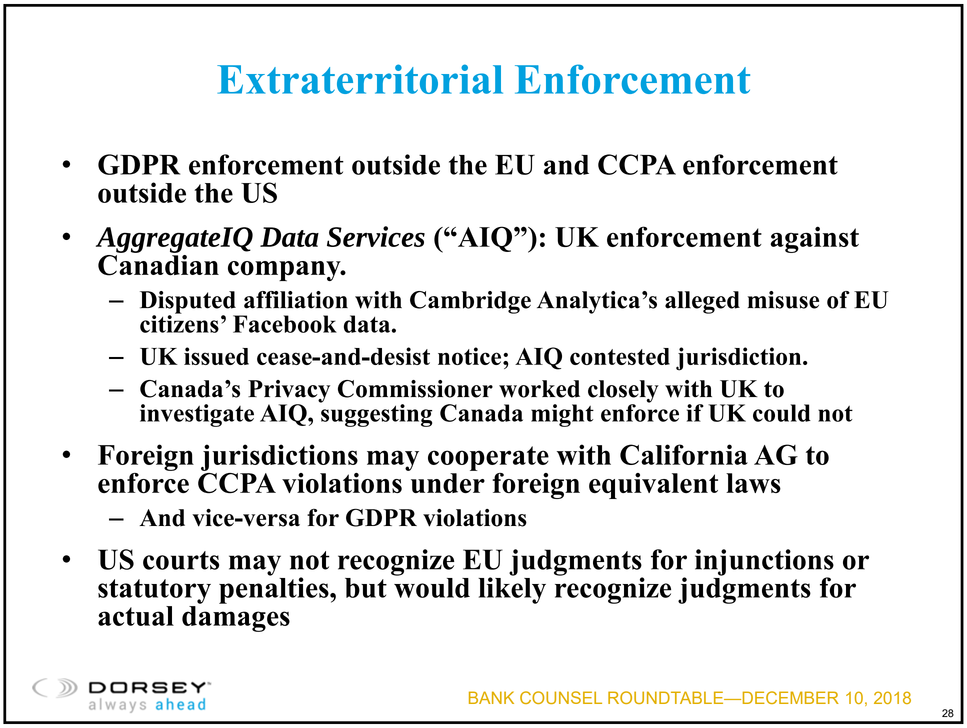
Key Differences—

- **Personal Information**: The CCPA defines personal information more broadly and includes “household” information
- **Notices, Policies, and Communication**: The CCPA provides greater detail on the information to be included in notices and privacy policies
  - The CCPA also specifies consumer must be able to communicate via toll-free number, and usually via website as well
- **Collection of Personal Information**: The GDPR requires
  - Opt-in permission
  - A legitimate interest, or
  - Limited other exceptions
  - The CCPA is not so limited
- **Geographic Location:** The GDPR regulates movement of covered data outside of the EU, whereas the CCPA applies restrictions without the same degree of geographic boundary restrictions
- **Sharing and Sale of Personal Information**: The CCPA imposes greater restrictions



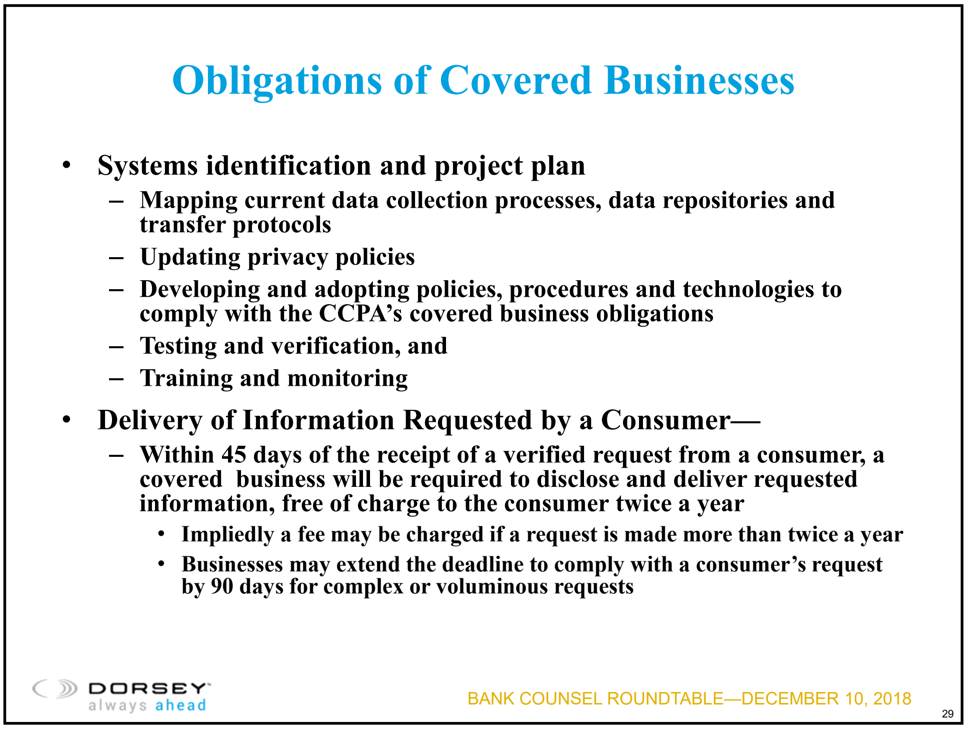
Implementation

- The CCPA is effective January 1, 2020
  - The California AG must issue regulations by July 1, 2020
  - No public enforcement until regulations are issued
  - *But* private right of action becomes effective on January 1, 2020
- The California Attorney General is authorized to issue regulations to implement the CCPA addressing—
  - Expanding the scope of coverage to encompass new technologies employed to capture consumer data
  - Expanded scope of new identifiers
  - Exceptions necessary to comply with state and federal laws
  - Procedures by covered business to comply with requests and directions for consumer information
  - Disclosures required to be provided
  - A uniform "opt-out" logo and button to be used on all websites
- All affected parties can request interpretative guidance from the California AG



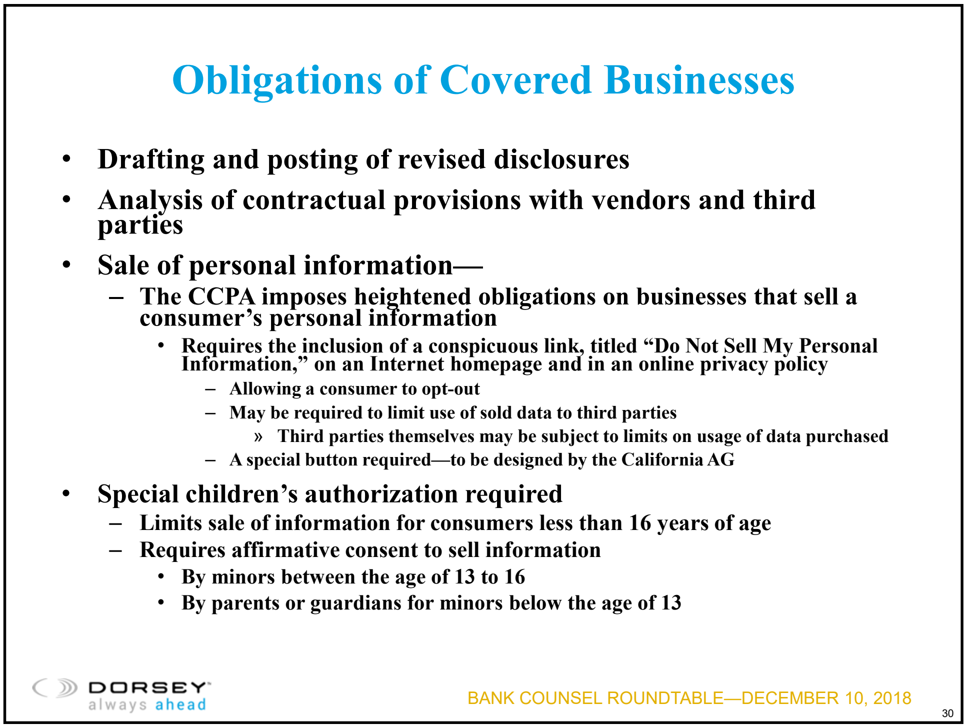
Extraterritorial Enforcement

- GDPR enforcement outside the EU and CCPA enforcement outside the US
- *AggregateIQ Data Services* ("AIQ"): UK enforcement against Canadian company.
  - Disputed affiliation with Cambridge Analytica's alleged misuse of EU citizens' Facebook data.
  - UK issued cease-and-desist notice; AIQ contested jurisdiction.
  - Canada's Privacy Commissioner worked closely with UK to investigate AIQ, suggesting Canada might enforce if UK could not
- Foreign jurisdictions may cooperate with California AG to enforce CCPA violations under foreign equivalent laws
  - And vice-versa for GDPR violations
- US courts may not recognize EU judgments for injunctions or statutory penalties, but would likely recognize judgments for actual damages



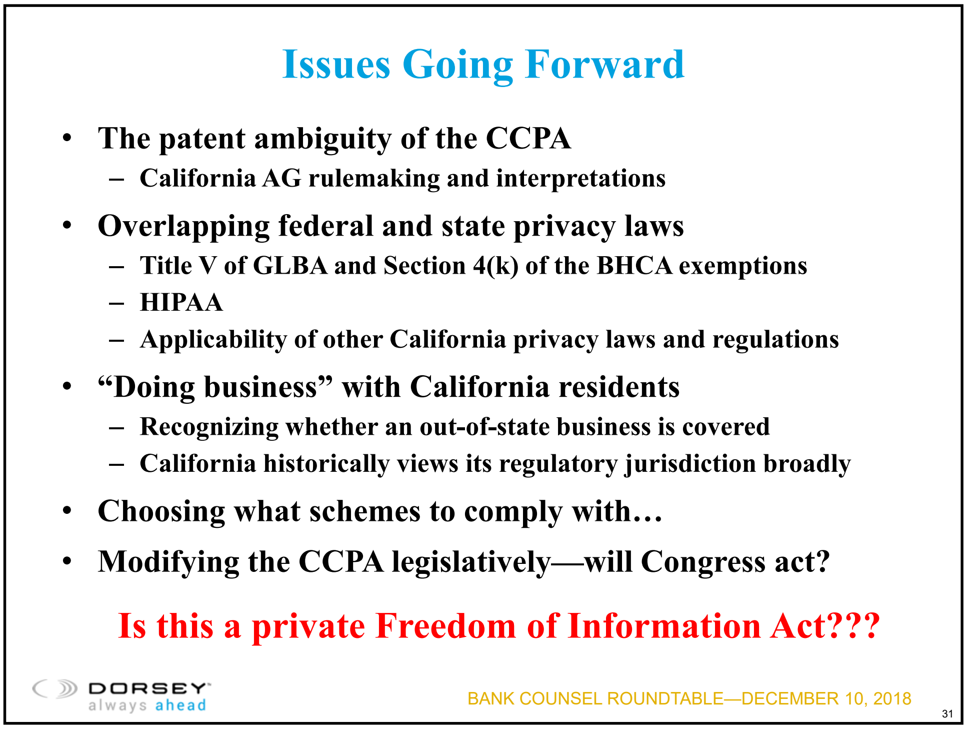
Obligations of Covered Businesses

- Systems identification and project plan
  - Mapping current data collection processes, data repositories and transfer protocols
  - Updating privacy policies
  - Developing and adopting policies, procedures and technologies to comply with the CCPA's covered business obligations
  - Testing and verification, and
  - Training and monitoring
- Delivery of Information Requested by a Consumer—
  - Within 45 days of the receipt of a verified request from a consumer, a covered business will be required to disclose and deliver requested information, free of charge to the consumer twice a year
    - Impliedly a fee may be charged if a request is made more than twice a year
    - Businesses may extend the deadline to comply with a consumer's request by 90 days for complex or voluminous requests



Obligations of Covered Businesses

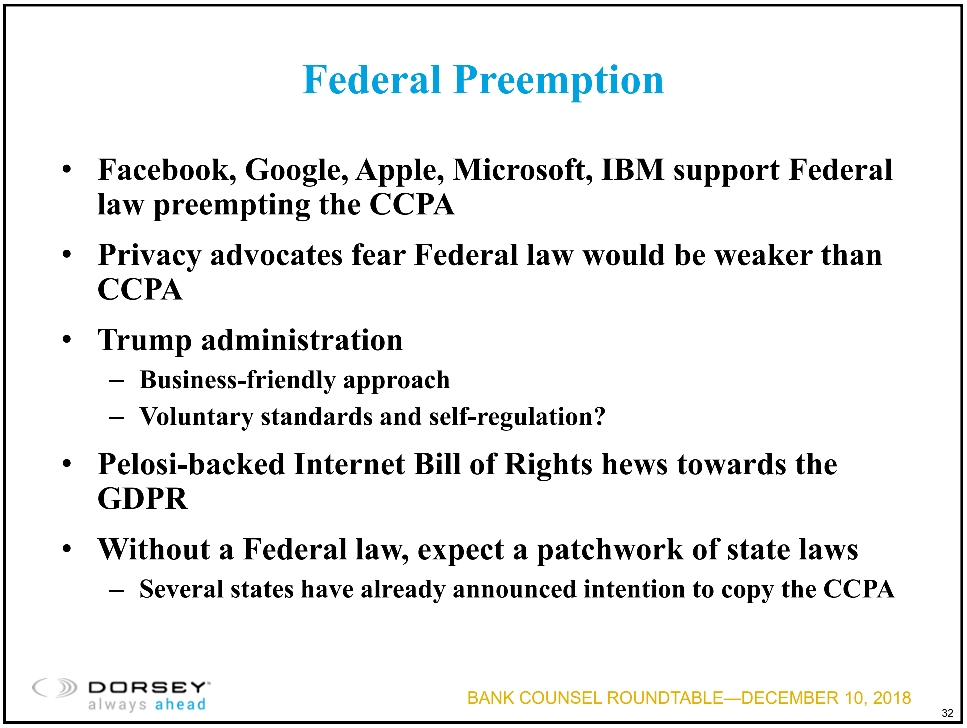
- Drafting and posting of revised disclosures
- Analysis of contractual provisions with vendors and third parties
- Sale of personal information—
  - The CCPA imposes heightened obligations on businesses that sell a consumer's personal information
    - Requires the inclusion of a conspicuous link, titled "Do Not Sell My Personal Information," on an Internet homepage and in an online privacy policy
      - Allowing a consumer to opt-out
      - May be required to limit use of sold data to third parties
        - » Third parties themselves may be subject to limits on usage of data purchased
      - A special button required—to be designed by the California AG
- Special children's authorization required
  - Limits sale of information for consumers less than 16 years of age
  - Requires affirmative consent to sell information
    - By minors between the age of 13 to 16
    - By parents or guardians for minors below the age of 13



Issues Going Forward

- The patent ambiguity of the CCPA
  - California AG rulemaking and interpretations
- Overlapping federal and state privacy laws
  - Title V of GLBA and Section 4(k) of the BHCA exemptions
  - HIPAA
  - Applicability of other California privacy laws and regulations
- "Doing business" with California residents
  - Recognizing whether an out-of-state business is covered
  - California historically views its regulatory jurisdiction broadly
- Choosing what schemes to comply with…
- Modifying the CCPA legislatively—will Congress act?

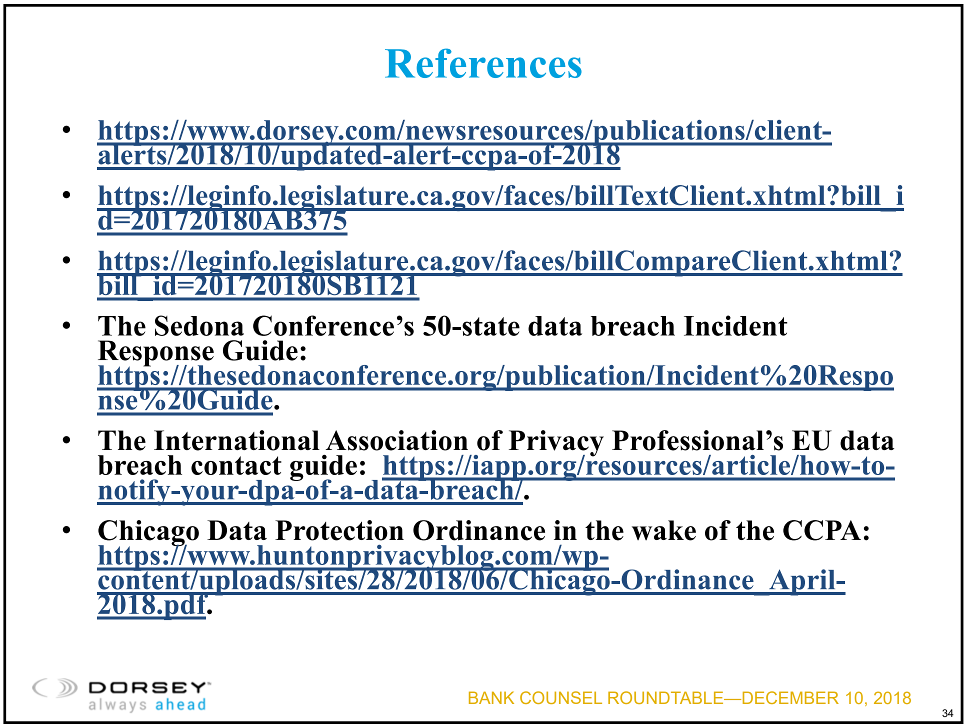
Is this a private Freedom of Information Act???



Federal Preemption

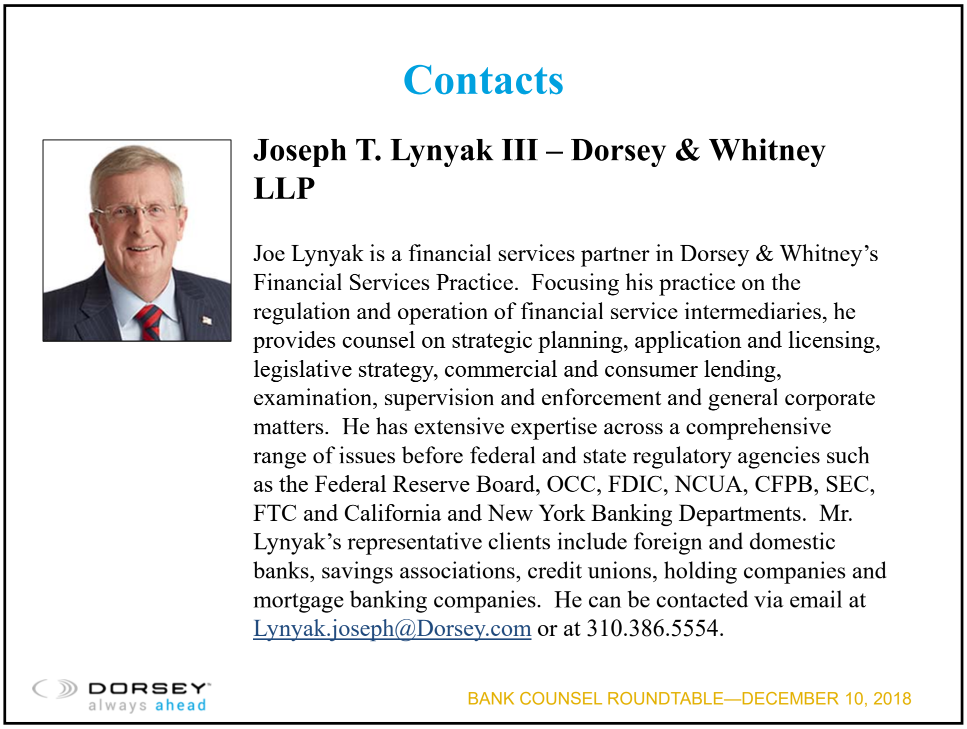
- Facebook, Google, Apple, Microsoft, IBM support Federal law preempting the CCPA
- Privacy advocates fear Federal law would be weaker than CCPA
- Trump administration
  - Business-friendly approach
  - Voluntary standards and self-regulation?
- Pelosi-backed Internet Bill of Rights hews towards the GDPR
- Without a Federal law, expect a patchwork of state laws
  - Several states have already announced intention to copy the CCPA

Questions???



References

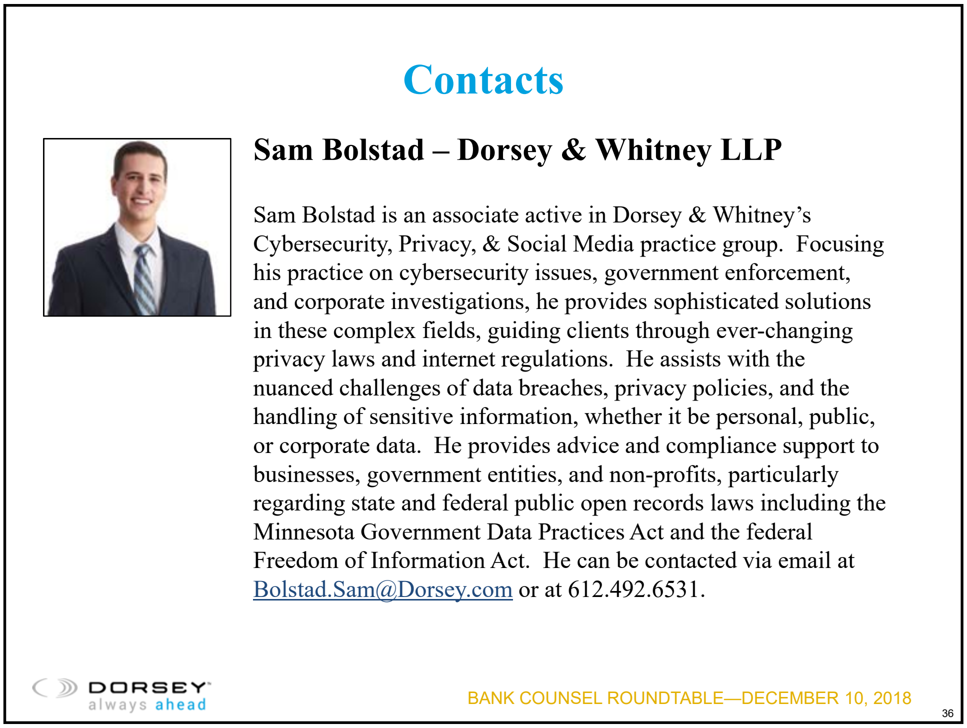
- https://www.dorsey.com/newsresources/publications/client-alerts/2018/10/updated-alert-ccpa-of-2018
- https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375
- https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180SB1121
- The Sedona Conference's 50-state data breach Incident Response Guide: https://thesedonaconference.org/publication/Incident%20Response%20Guide.
- The International Association of Privacy Professional's EU data breach contact guide: https://iapp.org/resources/article/how-to-notify-your-dpa-of-a-data-breach/.
- Chicago Data Protection Ordinance in the wake of the CCPA: https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2018/06/Chicago-Ordinance_April-2018.pdf.



Contacts

Joseph T. Lynyak III – Dorsey & Whitney LLP

Joe Lynyak is a financial services partner in Dorsey & Whitney's Financial Services Practice. Focusing his practice on the regulation and operation of financial service intermediaries, he provides counsel on strategic planning, application and licensing, legislative strategy, commercial and consumer lending, examination, supervision and enforcement and general corporate matters. He has extensive expertise across a comprehensive range of issues before federal and state regulatory agencies such as the Federal Reserve Board, OCC, FDIC, NCUA, CFPB, SEC, FTC and California and New York Banking Departments. Mr. Lynyak's representative clients include foreign and domestic banks, savings associations, credit unions, holding companies and mortgage banking companies. He can be contacted via email at Lynyak.joseph@Dorsey.com or at 310.386.5554.



Contacts

Sam Bolstad – Dorsey & Whitney LLP

Sam Bolstad is an associate active in Dorsey & Whitney's Cybersecurity, Privacy, & Social Media practice group. Focusing his practice on cybersecurity issues, government enforcement, and corporate investigations, he provides sophisticated solutions in these complex fields, guiding clients through ever-changing privacy laws and internet regulations. He assists with the nuanced challenges of data breaches, privacy policies, and the handling of sensitive information, whether it be personal, public, or corporate data. He provides advice and compliance support to businesses, government entities, and non-profits, particularly regarding state and federal public open records laws including the Minnesota Government Data Practices Act and the federal Freedom of Information Act. He can be contacted via email at Bolstad.Sam@Dorsey.com or at 612.492.6531.