WINSTON & STRAWN LLP

The California Consumer Privacy Act Is Here – What Happens Next?

January 29, 2020

Today's Webinar Presenters

Alessandra Swanson

Partner
Chicago
aswanson@winston.com

Sean Wieber

Partner
Chicago
swieber@winston.com

Eric Shinabarger

Associate
Chicago
eshinabarger@winston.com

Roadmap: Where We Are Headed Today

- High-Level Overview of CCPA
- Discussion of the Draft Regulations and Feedback to Date
- Additional Legislation That May Further Complicate the Landscape
- Enforcement of CCPA and Litigation-Related Risks
- Practical Scenarios: What To Do Now
  - All Businesses
  - Service Providers
  - Employers
  - Business-to-Business Organizations
  - Health Care Providers
  - Financial Institutions
  - Retailers/E-Commerce
  - M&A and PE Acquisitions

WINSTON & STRAWN LLP

Overview of CCPA

CCPA: Where Are We Now?

- Origins of CCPA
- Who is subject to the law?
  - Businesses
  - Service Providers
- Amendments passed in September 2018 and 2019
- Draft regulations released in October 2019
- California AG will not initiate enforcement actions until July 2020… but can look back to January to evaluate compliance

What Information Is Regulated?

- What constitutes “personal information”?
- What does this exclude?
  - Most notably:
    - Certain employment-related information
    - Certain business contact information
    - Protected Health Information regulated by HIPAA
    - Personal information collected, processed, sold, or disclosed pursuant to GLBA

WINSTON & STRAWN LLP

Draft Regulations

Implementing Regulations

- Draft regulations released in October 2019
- Final regulations expected in Spring 2020
- Draft Regulations:
  - Establish notice requirements for consumers
  - Create additional privacy policy requirements
  - Impose extensive requirements in connection with responding to individual rights requests
  - Enumerate verification requirements
  - Outline special rules related to minors
  - Describe non-discrimination provisions

Response to Draft Regulations

- Public comment period ran through December 2019
- Businesses potentially subject to the law submitted lengthy responses to the draft regulations, pointing out inconsistencies and noting that the regulations went well beyond the requirements of the law
- Final regulations are expected in spring 2020

What's Next for the CCPA?

- Additional changes will come, including:
  - Final provisions related to personal information collected in the employment and business-to-business context
  - Another ballot initiative to strengthen protections over sensitive personal information
  - The potential for a private right of action
- Also in 2020, the California Attorney General will likely initiate enforcement actions and (maybe) provide additional guidance on compliance expectations

WINSTON & STRAWN LLP

Additional Legislation

States Considering Privacy Legislation

- Several states have enacted more limited legislation governing online privacy practices (Nevada, Maine, several others pending)
- Others (e.g., Massachusetts and New York) would go beyond CCPA
- Four states have proposed CCPA copycats thus far in 2020
  - Includes Washington, which re-introduced a CCPA copycat in January 2020
  - Illinois Data Transparency and Privacy Act

WINSTON & STRAWN LLP

Enforcement of CCPA

Enforcement of CCPA

- The California Attorney General is the primary enforcer of CCPA
- The plaintiffs' bar will pursue actions connected to the private right of action for certain types of security breach
- There is also the potential for claims under state unfair competition laws
  - Plaintiffs (or regulators) may try to bring consumer rights suits against companies based on statements made in CCPA disclosures, or failures to comply with the CCPA's technical requirements
  - Plaintiffs will have to maneuver around the CCPA's disclaimer that it is not meant to confer a general private right of action
- The applicable statute of limitations period is unclear
- Federal Standing – is there a sufficiently concrete injury?

Attorney General Enforcement

- The California AG may bring enforcement actions
  - $2,500 for most violations; $7,500 for “intentional” violations
  - Penalty is for “each” violation
  - Not clear if “each” violation refers to each individual incident, or each affected record
    - Hypothetical: A business improperly sells personal information relating to 1,000 consumers. $2,500 or $2,500,000?
    - Likely the latter

CCPA's Private Right of Action

- There is a private right of action for data breaches for info protected under breach law
  - Failure to implement "reasonable" security procedures and practices to protect information
  - Must provide opportunity to "cure"
  - Consumers may seek the higher of actual damages or up to $750 per incident
  - This private right of action applies to employee data
- Availability of statutory damages likely to increase class actions
  - Data breaches typically face limited class action interest outside of the biggest breaches
  - It is difficult to prove actual damages

WINSTON & STRAWN LLP

Practical Scenarios

All Businesses

Data Mapping:

- Understand how personal data flows into, through, and out of your organization
- This is critical to understanding:
  - Where personal data “lives” so your organization can accurately act on individual rights requests
  - Identify how “sensitive data” subject to CA’s breach law is protected
  - Determine if there are any unintentional or intentional “sales” of personal information
- Understand who “owns” these processes, what third parties are receiving this data, and what contracts govern these relationships

All Businesses

Contract Review:

- Understand what third parties are receiving your personal data and what rights they have to it
- Talk to your business teams about the contracting process and raise awareness about the implications of sharing personal data
- Take steps to ensure that risk is properly accounted for in contracts, or if that is infeasible, that there are other ways to protect the organization (e.g., cyber insurance)

All Businesses

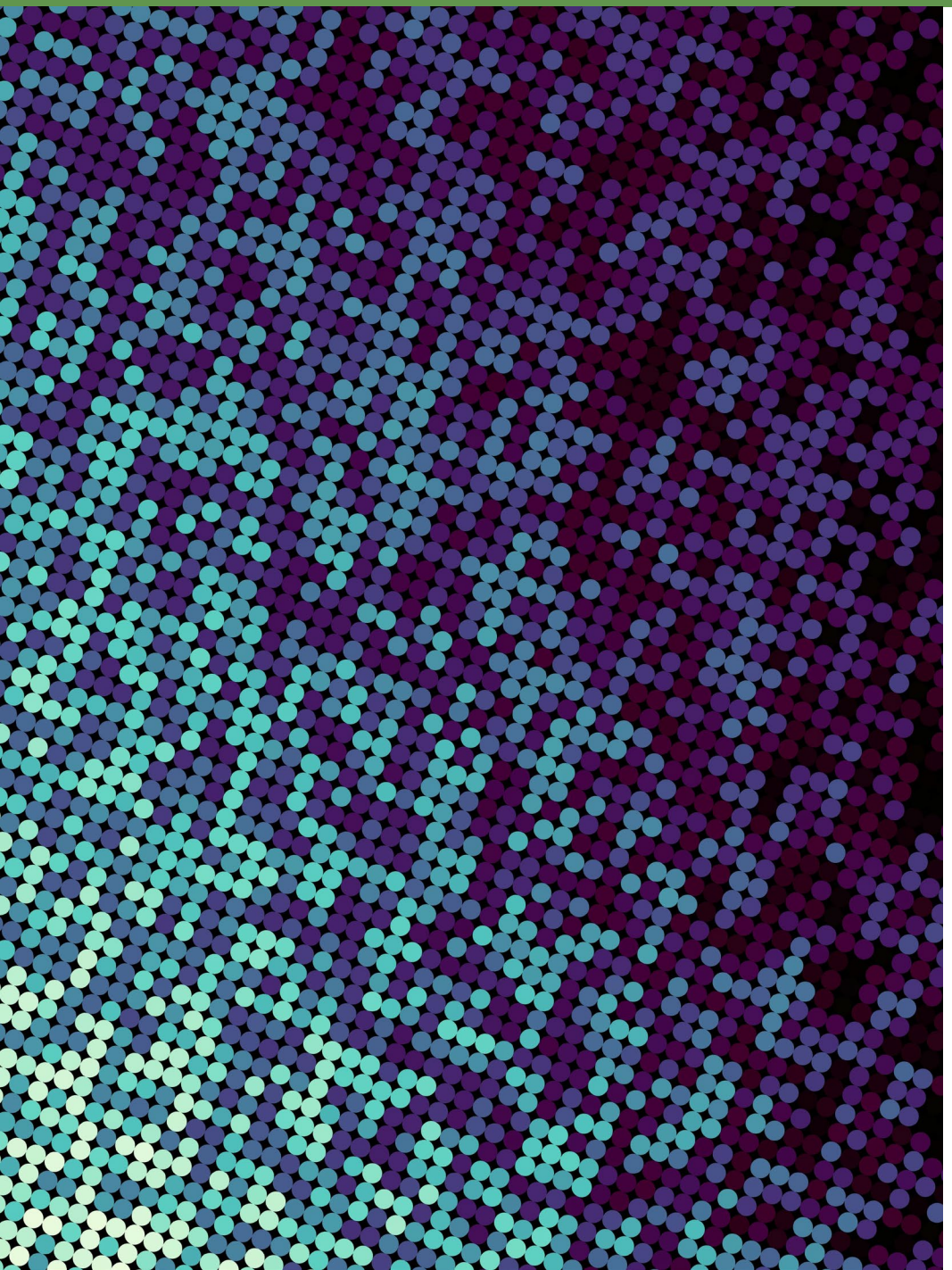
Get organized internally:

- How will individual rights requests be received by the organization?
- How will the organization verify consumer identities?
- Who will process them?
- Who is in charge of keeping data maps up to date?
- Which “process owners” will conduct the diligence for the requests?

All Businesses

Review data security practices:

- Ensure sensitive personal data is appropriately protected
- Educate individuals who “touch” personal data about new obligations under CCPA
- Establish or strengthen information security program infrastructure
  - Who is in charge?
  - Are appropriate policies and procedures in place?
  - How often are security assessments undertaken?
  - Think of potential defenses to data security class actions



All Businesses

Update Privacy Notices

- Balancing obligations to disclose online/offline practices in California vs. online practices for the rest of the country
- Disclosing whether or not personal data is "sold"
- Structuring the policy to address the California requirements
- Describing individual rights and request procedures

Service Providers

- Determine the extent to which your organization is a “business” vs. a “service provider”
- Examine customer contracts to ensure you have appropriate rights to data to complete necessary R&D
- Create an addendum to address your obligations under CCPA
- Talk to your customers to establish expectations
- Create internal processes to address individual rights requests

Employers

- Focus is on creating and making available a privacy notice related to the treatment of employment-related personal information
- Talk to your organization's internal and external recruiters to understand how they are "touching" personal information
- Review vendor agreements to understand how sensitive personal information is protected (especially if the agreement is older than five years)
- Review cyber insurance coverage

Business-to-Business

- The exception can be broadly or narrowly interpreted; discuss internally to best understand your organization's risk tolerance here
- Consider all online and offline processes that lead to the collection of personal information in the business context
- Assess whether any personal information collected in this context is "sold"
- Confirm appropriate data security measures are in place

Health Care Providers

- While PHI is fully exempt (even from the private right of action), other personal information collected by your organization may be subject to CCPA
- This includes employment-related information, information collected through websites, and fundraising information
- Determine whether non-profit status will affect compliance obligations
- While PHI is not subject to the private right of action, other information typically collected in the course of providing services to patients (e.g., credit card information for a third party paying for health care services on behalf of a patient) may be subject to CCPA
- Address de-identification discrepancies

Financial Institutions

- GLBA-covered personal information is exempt from many provisions of the law, but is still subject to the private right of action for certain types of security breach
- Examine what other types of personal information under your organization's purview may be affected by CCPA
- Understand what adjustments may need to occur on your organization's website (e.g., updated privacy notice and consent language)

Retail and E-Commerce

- For retail, heavy focus on what is happening in-store
  - What personal information is collected?
  - How can your organization make the privacy notice available?
  - How is information collected (in writing, through a tablet, etc.)?
- For e-commerce, is your organization placing consent language on your site at all areas of information collection? Is the privacy policy properly made available?
- Is your organization's business team aware of the change in regulation and how it may impact marketing and consumer reach?
- Does your organization have effective processes in place to ensure that no actions are taken in violation of the privacy policy?

M&A and PE Transactions

- Privacy diligence has become more complicated, especially since more laws have private rights of action attached to them
- Increased emphasis on privacy risk from underwriters and insurers, which can lead to RWI policy exclusions and the need for escrows or special indemnities in transactions
- Additional investment in new acquisitions and portfolio holdings in order to minimize risk throughout life of investment
- To avoid complications upon exit, be proactive about privacy and security compliance obligations

Thank You

Alessandra Swanson

Partner
Chicago
aswanson@winston.com

Sean Wieber

Partner
Chicago
swieber@winston.com

Eric Shinabarger

Associate
Chicago
eshinabarger@winston.com