Getting Ahead of the CCPA: How to Unravel and Master the Complexities

NEW YORK | WASHINGTON DC | NORTHERN VIRGINIA | CLEVELAND | CHICAGO | MINNEAPOLIS | LOS ANGELES | SAN FRANCISCO

Speakers

David C. Shonka
Partner, Washington, D.C.

Karin S. Jenson
Partner, Cleveland

Ambre N. McLaughlin
Counsel, Northern Virginia

Today's Webinar

Basic Concepts

Recent Amendments & Complexities

Building a Compliant Program, Brick-by-Brick

Basic Concepts

- The CCPA: A collection of simple, long-recognized principles that are mired in complexities
- Mastering the complexities requires building a strong program, one brick at a time

CCPA's Simple Principles

Fundamental Consumer Rights

- Consumers have a right to know and a right to access to their data
- They have a right to opt-out of sales
- They also have a right to request deletion
- **Businesses cannot discriminate against consumers who exercise these rights**

Many antecedents

- Fair Information Practice Principles
- Fair Credit Reporting Act
- Access to medical records

The 2019 Amendments

- Some clarifications
  - Definition of personal information to clarify “reasonably” standard
  - **CCPA does not apply** to FCRA-covered information
  - Makes other exclusions clear
- Some complexities give temporary, *partial* carve-outs to:
  - Data collected from job applicants, employees, owners, officers, medical staff, and contractors
  - Data collected from consumers acting solely on behalf of another business
- Two that are for another day
  - Vehicles
  - Data brokers

Businesses Have Many Issues To Address

- Scope of personal data
- Linking collected data to 11 categories of data
- Multiple exceptions to the obligation to delete
- Dealing with minors
  - Are they between the age of 13 and 16?
  - Are they under the age of 13?
- Distinguishing categories of sources of information
- How to tie collected categories of information to categories of sources and categories of recipients
- What is a business purpose?
- What is a commercial purpose?
- Who is a service provider?
- Who is a third party?
- How are requesters to be verified?
- What is a sale?
- What is sharing?
- Separating job applicants, employees, owners, officers, medical staff, and contractors from other consumers
- Separating business-to-business consumers from other consumers
- What is discrimination?
- What is not discrimination?
- How is personal data valued?
- When is personal information not personal?
- What is household information?
- Who owns household information?
- How is it all linked together for production?
- Etc., etc., etc.

AG's Proposed Regulations

- It is prudent to approach them as if they will be the final regulations
- The proposals provide many useful clarifications
- They fill in several blanks

AG's Proposed Regulations (cont'd.)

1. Clarify disclosures
   - Proposed 11 CCR 999.301(n) clearly identifies 6 information points for disclosures
2. Clarify content of important notices
   - "Notice at Collection"
   - "Notice of Right to Opt-Out"
   - "Notice of Financial Incentives"
   - The Privacy Policy

AG's Proposed Regulations (cont'd.)

3. Delineate procedures
   - Submitting and responding to "Requests to Know"
   - Submitting and responding to "Requests to Delete"
   - Submitting and responding to "Requests to Opt-Out"
4. Give content to verification requirements
   - Set general principles and strict prohibitions
   - Give specific guidance for
     - Password-protected accounts
     - Non-account holders
     - Authorized agents
     - Children
     - Households

Building A Compliant Program, Brick by Brick

- Milestones in the program's construction
  - Completing the data map
  - Developing a verification process
  - Preparing and posting required notices
  - Vesting the right person with the necessary powers – and budget
  - Creating and maintaining a culture of compliance
  - Preparing and implementing a process for dealing with consumer requests
  - Reviewing existing and new contracts
  - Being ready for the future

Building A Compliant Program, Brick by Brick

- Create a comprehensive PI data map
  - Identify locations (one at a time) where PI is located
    - Servers
    - Devices
    - Cloud environments and applications
    - Note: The data map must identify all locations where data is found in order to comply with any request to delete
  - Identify each source of PI on each site
    - Customers
    - Employees, job applicants, owners, officers, medical staff, contractors
    - B2B transactions and communications
    - Other businesses
    - Public Information

Building A Compliant Program, Brick by Brick

- Develop verification process
  - As required in Proposed Regulations (e.g., 11 CCR Article 4)

    Proposed Regulations set out detailed requirements
    - 11 CCR 999.323 (general rules)
    - 999.324 (password-protected accounts)
    - 999.325 (non-account holders)
    - 999.326 (authorized agents)
    - 999.330(a)(1) and (2) (adopting COPPA requirements for verification and adding affirmative consent)
    - See 999.318 (concerning households)
    - Observe additional requirements when verification is not possible
- Develop or revise current privacy policy
  - As required by Proposed Regulation (11 CCR 999.301(b))

Building A Compliant Program, Brick by Brick

- Prepare required notices
  - Right to Know

    Notice at Collection
    - Be aware of limitation on undisclosed uses
    - Maintain requisite records (11 CCR 999.305(d)(2))

    Request To Know (11 CCR 999.312 and 313)

    Request to Delete (11 CCR 999.312 and 313)
  - Notice of Right to Opt-out (11 CCR 999.306)
  - Notice of Financial Incentives (11 CCR 999.307)

Building A Compliant Program, Brick by Brick

- The compliance or privacy officer
  - Allot sufficient resources
    - This is a corporate budget item
  - Qualified person
    - Understanding of privacy issues and risks
    - Experience in managing people, programs, and resources
  - Direct access to senior executive, and authority to make binding decisions
  - Defined responsibilities and accountability
    - Developing and implementing the program
    - Execution and compliance
    - Training and record-keeping
    - Review and refresh

Building A Compliant Program, Brick by Brick

- Establish a culture of compliance
  - Top to bottom / across silos
  - Privacy by design
  - Privacy impact assessments
  - Gap analyses
  - Improve and remediate

Building A Compliant Program, Brick by Brick

- Dealing with Consumer Requests
  - Authenticate requester
  - Channel requests to the response team
  - Retrieve all PI covered by the request
  - Review collected material
  - Categorize information and respond to request
  - Provide required disclosures when denying a request
  - Follow up with consumer, if needed

Building A Compliant Program, Brick by Brick

- Contract review
  - Coordinate with legal
    - Review and amend third-party contracts
  - Are you a retaining a service provider?
    - What is a service provider?
    - Does the contract require compliance?
  - Are you a service provider?
    - Do you understand your responsibilities?
    - Are you complying with them?

Maintaining the Structure

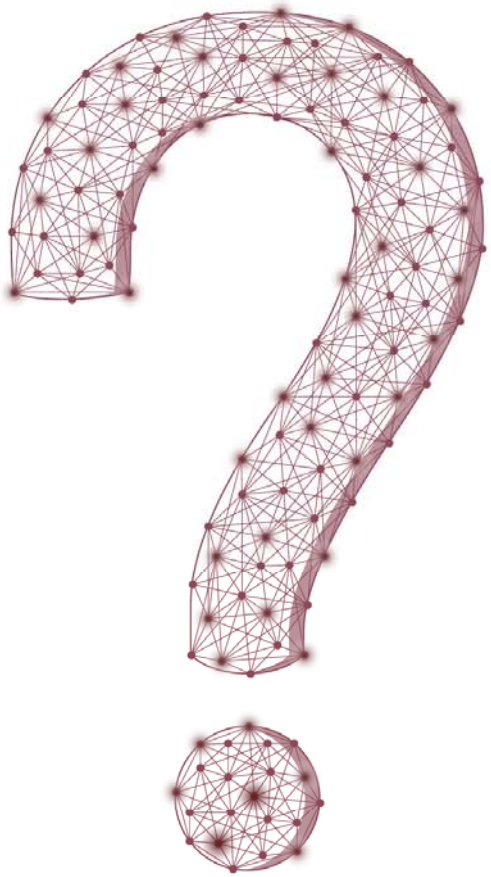
- This is the beginning, not the end, of the process
  - Gaps and flaws will be exposed
  - New technologies and uses for information will evolve
  - Existing laws will be amended
  - Future laws will be enacted
  - The program must be dynamic, not static

Conclusion

Two Months to Go:

Are You Ready for January 1st?

And beyond?



QUESTIONS?

Thank you!

David C. Shonka
dshonka@redgravellp.com
202-384-6348

Karin S. Jenson
kjenson@redgravellp.com
216-210-1954

Ambre N. McLaughlin
amclaughlin@redgravellp.com
703-592-1398