Drinker Biddle®

California Consumer Privacy Act Overview

The California Consumer Privacy Act of 2018 ("CCPA" or "the Act") takes effect on January 1, 2020.

KEY DEFINITIONS

Despite its name, the CCPA applies to a broader class of individuals than colloquial understandings of "consumers." The term "consumer" is defined under the Act, in relevant part, as "a natural person who is a California resident." Thus, customers, employees, business contacts, and others are protected individuals under the Act.

"Personal Information" is broadly defined under the CCPA and includes a number of enumerated categories of personal information. In general, information that can be linked to a person, device, or browser will be considered "personal information."

KEY REQUIREMENTS

The CCPA empowers CA residents with the following six data privacy rights:

1. To be provided with information on what personal information is collected about them and the purposes for which that personal information is used.
2. To be provided with information on what personal information is sold or disclosed for a business purpose and to whom.
3. To opt out of the sale of their personal information to third parties (or in the case of minors under age 16, to require an opt in before the sale of their personal information).
4. To request the deletion of their personal information.
5. Not to be subject to discrimination for exercising any of the above rights, including being denied goods or services or being charged a different price, or being subjected to a lower level of quality, of such goods or services.
6. To seek statutory damages of $100 to $750 for breaches of unencrypted personal information that arise as a result of a business' violation of its duty to implement and maintain reasonable security procedures.

The CCPA also requires that a business must in its online privacy policy, or in a California-specific privacy policy posted on its website, describe CA residents' rights to request information and list the categories of CA residents' personal information it has in the prior 12 months (i) collected, (ii) sold, and (iii) disclosed for business operational purposes.

In addition to describing the right to opt-out in its online privacy policy or California-specific privacy policy, a business must include a "clear and conspicuous" link on its homepage to a web page where individuals can exercise their opt out rights. The link must be titled "Do Not Sell My Personal Information" and must link to a page with the same title.

Preparing for CCPA Compliance: Security, Incident Prevention, and Strategic Response

Presenters:
Pete Baldwin
Peter.Baldwin@dbr.com

Jason G. Weiss
Jason.Weiss@dbr.com

CCPA Webinar #7
September 24, 2019

Drinker Biddle

Webinar Schedule

1:00 – 2:00 PM US Eastern

- Today
- October 30, 2019
- December 4, 2019

Let us know what topics you would like us to focus on in the upcoming webinars!

Introduction & Overview

- CCPA – Why should you care?
  - Enforcement:
    - Private Right of Action (§ 1798.150)
    - Attorney General Enforcement (§ 1798.155)
- Tips to prepare for the CCPA and avoid future litigation and/or enforcement penalties

CCPA Private Right of Action

- The CCPA provides for a narrow private right of action for data breaches involving certain categories of unencrypted and unredacted personal information
  - Amendment with broader private right of action was not passed
- Private right of action applies to breaches of "personal information" as defined under California's general data security statute (Cal. Civil Code § 1798.81.5)
  - Comparatively narrow definition of "personal information"
    - An individual's first name or first initial and last name in combination with any one or more of the following: SSN; driver's license number or CA 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; health insurance information
    - Username or email address in combination with a password or security question and answer that would permit access to an account

CCPA Private Right of Action

- Available Relief under the CCPA:
  - Impacted consumers may bring a civil action for any of the following:
    - Damages
      - Statutory damages: $100 - $750 per consumer, per incident; or
      - Actual damages (if greater than the statutory damages amount)
    - Injunctive or declaratory relief
    - Any other relief the court deems proper
  - Actions for damages may be brought on an individual or class basis
  - Private actions are available to impacted consumers beginning on January 1, 2020

CCPA Private Right of Action

- Relevant circumstances to be considered by the court when assessing statutory damages:
  - Nature and seriousness of misconduct
  - Number of violations
  - Persistence of misconduct
  - Length of time over which the misconduct occurred
  - Willfulness of the misconduct
  - Defendant's assets, liability and net worth

CCPA Private Right of Action

- Prior Notice
  - Before bringing an action for statutory damages, a consumer must provide the business with 30 days written notice of the violation, identifying "specific provisions of this title" the consumer will allege the business has violated
    - If the business can cure the violation within 30 days and provide the consumer with an express written statement that the violations have been cured and no further violations will occur, a consumer/class may not seek statutory damages
    - If the business violates the terms of its express written statement, then the consumer/class may pursue an action to "enforce" the written statement and may claim statutory damages for each violation . . . as well as any other violation of the CCPA that postdates the written statement
  - Note, however, that a consumer is <u>not</u> required to provide notice if seeking <u>actual</u> damages

CCPA Attorney General Enforcement

- The Attorney General may bring a civil action against any business, service provider, or other person who violates the CCPA
  - Not limited just to data breaches
- A business will be in violation of the CCPA if it fails to cure any alleged violation within 30 days of being notified of its non-compliance
- The Attorney General will not begin to enforce the CCPA until 6 months after the final regulations are published or July 1, 2020, whichever is sooner
- A business or third party may seek the opinion of the Attorney General for guidance on how to comply with the CCPA

CCPA Attorney General Enforcement

- Penalties:
  - The Attorney General may seek an injunction and
  - Each violation may result in a civil penalty of up to $2,500
  - Each intentional violation may result in a civil penalty of up to $7,500
- Depending on judicial interpretation, fines could grow exponentially
- Civil penalties shall be exclusively assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General
- Penalties deposited in the Consumer Privacy Fun to offset any costs incurred by the state courts and the Attorney General in connection with the CCPA

CCPA Enforcement Predictions

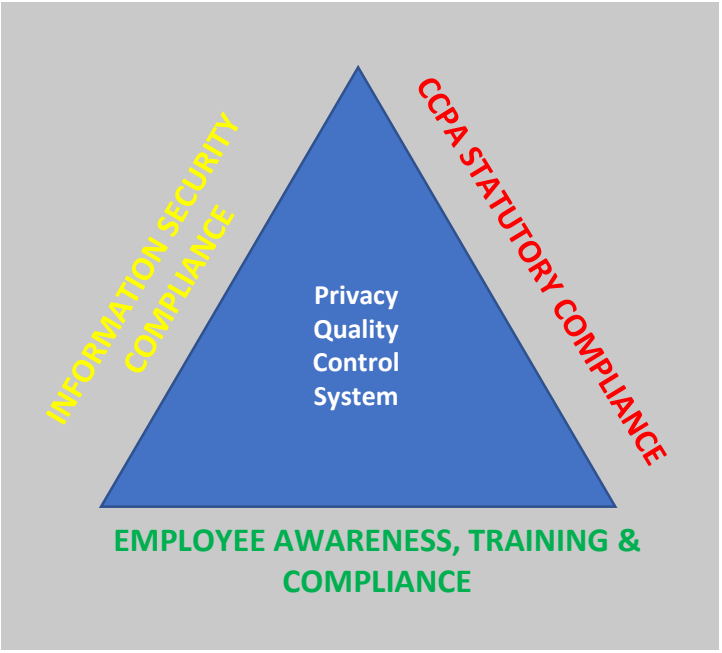
- Enforcement by the Attorney General will not begin until July 1, 2020
- How well-equipped is the Attorney General's Office to handle the likely flood of complaints?
  - According to testimony by the Attorney General's Office before the California State Senate, there will be an increase in budget and headcount starting in 2020 specifically devoted to CCPA enforcement
  - At present, the Attorney General's Office has limited resources and, as a result, a limited ability to prosecute cases under the CCPA
  - At the outset, the Attorney General's Office is likely to focus on a few big name targets and/or particularly egregious cases that will result in significant publicity and fines
    - The initial fines will provide additional resources to allow the Office to settle into a more predictable enforcement pattern in 2021 and beyond

CCPA Enforcement Predictions

- GDPR enforcement as a model for CCPA enforcement?
  - Initial enforcement focus on companies that suffered a data breach
  - But subsequent enforcement moves beyond data breaches – less reactively punitive and more proactively preventative
  - Impossible to institute enforcement proceedings for every breach
  - Initial splash with big name target and fine – Google ($50 million)
  - Notwithstanding Google, fines have been relatively modest, but the total dollar amount of the fines is significant (almost $400 million)
    - Volume of enforcement actions is increasing (~80 to date)
  - As the number of complaints increases, so too will enforcement (it takes time for enforcement authorities to catch up)
- General trend towards more active state enforcement
  - Joint enforcement actions will continue to proliferate

Three-Pronged Privacy Quality Control System

- Ensures both short- and long-term compliance with CCPA requirements
- If one prong is weak or fails, CCPA compliance fails and you can be exposed to potential liability



Phased Approach to CCPA Preparation

- Eight phases of preparation and compliance
  - Phase 1: Initial preparation
  - Phase 2: Initial assignments
  - Phase 3: Statutory conformance
  - Phase 4: InfoSec conformance
  - Phase 5: Employee training
  - Phase 6: Conformance assessments
  - Phase 7: CCPA conformance review
  - Phase 8: Long-term conformance

CCPA 2020

Phased Approach to CCPA Preparation

- Phase 1: Initial Preparation
  - Identify key personnel within your organization
  - Identify a management point of contact
  - Identify a day-to-day point of contact
  - Identify team leaders and members, both inside and outside of the organization (e.g., outside counsel, consultants, vendors, etc.)
  - Identify IT points of contact within the organization

- Phase 2: Initial Assignments
  - Assign tentative team and roles for each phase of the project
  - Structure the project's goals and timelines

Phased Approach to CCPA Preparation

- Phase 3: Statutory Conformance
  - Create CCPA compliance policies
  - Review policies for conformance with statutory requirements
  - Determine if there is a need for corrective action or remediation

- Phase 4: InfoSec Conformance
  - Create CCPA InfoSec compliance policies
  - InfoSec compliance review
  - Compare against NIST standard
  - Determine if there is a need for corrective action or remediation

Phased Approach to CCPA Preparation

- Phase 5: Employee Training
  - Create CCPA-specific trainings and incorporate into policies/procedures
  - Prepare employees to recognize issues and understand compliance requirements
  - Work with outside counsel and/or vendors to ensure adequacy of training

- Phase 6: Conformance Assessment
  - Work with outside counsel and/or vendor to review CCPA conformance records
  - Provide all relevant records for review
  - Make employees available for interviews
  - Determine if there is a need for corrective action or remediation

Phased Approach to CCPA Preparation

- Phase 7: CCPA Conformance Review
  - Review all aspects of CCPA preparation and compliance with key internal and external points of contact and responsible individuals
  - Analyze effectiveness of trainings and policies
  - Begin to focus on long-term strategy for ongoing conformance

- Phase 8: Long-Term Conformance
  - Work with stakeholders to create a long-term plan to ensure CCPA compliance
  - Schedule routine self-audits and external assessments for all aspects of CCPA compliance
  - Establish and implement corrective action plan
  - Conduct routine surveillance assessments
  - Update policies and procedures to meet ongoing obligations

CCPA Preparation Tips

- Top 10 Things Companies Should be Doing to Prepare:
  - Start preparing NOW
  - Designate a specific person to coordinate planning for CCPA
  - Read the statute – don't be afraid to get help if you don't understand
  - Inventory your business data ASAP – know what you've accumulated
  - Create a "data map" to know where data is on your network
  - Consider encrypting your data
  - Start planning a CCPA-compliant website and/or toll-free number
  - Ensure that IT personnel have security hardware/software configured
  - Ensure that your CCPA policies are properly documented and distributed to employees
  - Start training your employees NOW

CCPA Preparation Tips

- Top 10 CCPA Preparation Mistakes:
  - Waiting and praying that the CCPA will go away
  - Not getting CCPA compliance team and leadership in place
  - Not ensuring data inventory and data security procedures are in place and working
  - Having customer data spread out over too many locations on network
  - Not creating a system to respond to verified customer requests
  - Not conducting thorough self assessments
  - Not actually reading the CCPA
  - Not having a centralized repository for CCPA policies
  - Not thinking about the CCPA as a long-term obligation
  - Not asking for help when you need it

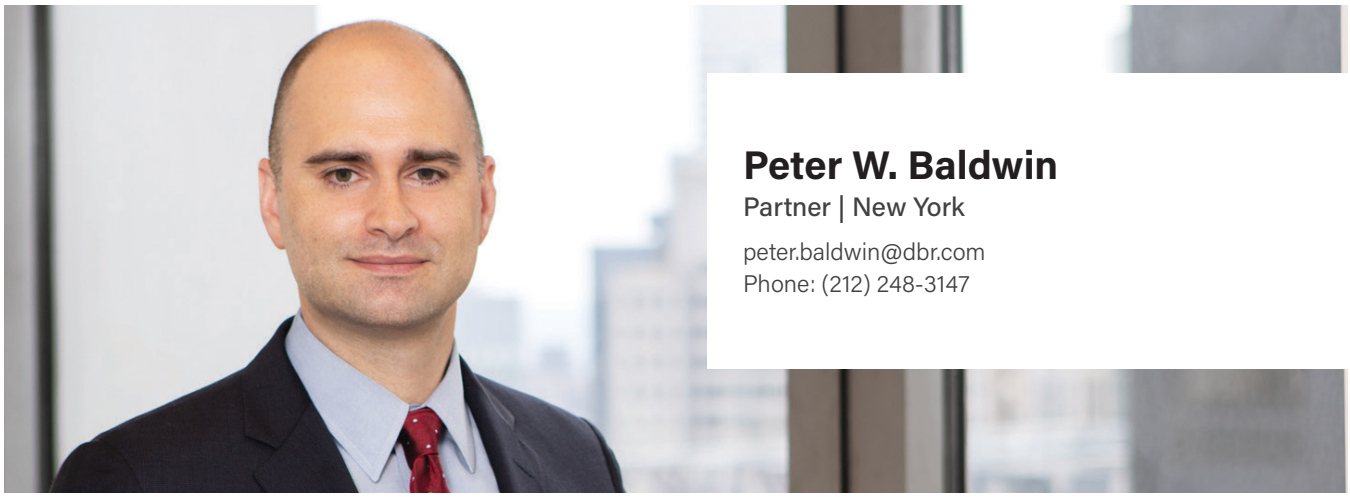
Contact Information

Pete Baldwin
Drinker Biddle & Reath LLP
1177 Avenue of the Americas, 41st Floor
New York, New York 10036
(212) 248-3147
Peter.Baldwin@dbr.com

Jason G. Weiss
Drinker Biddle & Reath LLP
1800 Century Park East, Suite 1500
Los Angeles, California 90067
(310) 203-4062
Jason.Weiss@dbr.com

Questions?

DrinkerBiddle®



Peter W. Baldwin

Partner | New York

peter.baldwin@dbr.com
Phone: (212) 248-3147

About

Peter W. Baldwin draws on his experience as a former federal prosecutor in New York and California to counsel clients facing government and internal investigations, securities enforcement actions, cybersecurity issues, and other complex civil and criminal litigation matters. Pete works with businesses, executives, boards of directors, and other decision-makers to respond to government inquires and to craft policies and procedures that will help them stay compliant in an increasingly regulated business environment.

Pete advises clients with responding to both civil and criminal government inquiries and investigations, regularly liaising with multiple federal and state agencies and regulators. He represents both individual and corporate targets, subjects, and witnesses, and provides guidance about responding to unofficial inquiries, subpoenas, search warrants, and requests for interviews and grand jury testimony. Pete has also prepared clients to testify in civil and criminal court proceedings.

Pete works with clients before, during, and after cybersecurity incidents, and his experience as a former federal cybercrime prosecutor has proven invaluable for clients in the areas of forensic analysis, breach remediation, victim notification, and responding to inquiries by regulators and law enforcement agencies. He has counseled clients facing a wide array of cybersecurity, data privacy, and data security issues, including network intrusions, business email compromise scams, malware, and ransomware. His work has included determining whether and when it is appropriate to seek the assistance of law enforcement authorities; in the course of such engagements, he has helped clients develop valuable relationships and contacts with law enforcement agencies.

Clients also turn to Pete for representation in complex civil matters. He has litigated civil cases involving RICO and fraud charges, as well as high-stakes, multimillion dollar mediation and arbitration proceedings.

Prior to joining Drinker Biddle, Pete spent over eight years as an Assistant United States Attorney in the U.S. Attorney's Offices for the Eastern District of New York and Central District of California. In this role, he supervised all aspects of criminal investigation and prosecution, first as a member of the Major Frauds Section in the Central District of California and then in the National Security and Cybercrime Section in the Eastern District of New York.

As a federal prosecutor, Pete worked extensively with numerous federal law enforcement and regulatory agencies to oversee grand jury investigations, criminal charging decisions, plea negotiations, motions practice, evidentiary hearings, trials, sentencing proceedings, and appeals. Pete has served as lead trial counsel in multiple criminal jury trials. During his time with the Eastern District of New York's National Security and Cybercrime Section, Pete directed federal criminal investigations involving cybercrimes, export controls, terrorism, trade secrets, BSA/AML violations, and money laundering. In addition, Pete served as the EDNY's Counterespionage and Export Controls Coordinator. In this role, he directed the investigation and prosecution of cases relating to violations of federal export controls, counter proliferation, trade secrets and espionage laws, and he also served as the Office's primary point of contact with various federal law enforcement and regulatory agencies, as well as with the U.S. intelligence community. Prior to that, in the Central District of California's Major Frauds Section, Pete prosecuted cases involving securities fraud, wire fraud, tax fraud, health care fraud, the Foreign Corrupt Practices Act, and money laundering.

Prior to his work as an Assistant U.S. Attorney, Pete practiced commercial litigation at a major international law firm in Los Angeles, handling matters including securities fraud, derivative actions and business disputes.

DrinkerBiddle®

Areas of Focus

Services

- Litigation
- Commercial Litigation
- White Collar Defense and Corporate Investigations
- Trade Secrets
- Cybersecurity and Incident Response Services

Industries

- Enterprise Blockchains, Smart Contracts and Distributed Ledger Technology

Credentials

Bar Admissions

- California
- District of Columbia
- New York

Education

- Northwestern University School of Law, J.D., 2006, *cum laude*, Order of the Coif, Note & Comment Editor, *Journal of Criminal Law & Criminology*
- Yale University, B.A., 2000

DrinkerBiddle®

Jason G. Weiss

Counsel | Los Angeles

jason.weiss@dbr.com
Phone: (310) 203-4062

About

Jason G. Weiss is an attorney and award-winning law enforcement and cybersecurity professional who served with distinction for over two decades at the Federal Bureau of Investigation. He is Counsel in Drinker, Biddle and Reath's Information Governance and E-Discovery group, where his practice focuses on cybersecurity incident preparedness and response, compliance with CCPA and other information governance laws and requirements, as well as data analytics, investigations, and e-discovery.

Prior to joining Drinker Biddle, he was most recently a Supervisory Special Agent in the FBI Los Angeles Cyber and Forensics branch, where he founded, designed, and lead a nationally-recognized and accredited computer forensics laboratory. With deep expertise in the management of data breaches, computer intrusion, cybercrime, forensic investigation, white collar crime, counterintelligence, and counterterrorism, Jason also provided FBI-wide legal, technical, and management expertise in connection with hundreds of nationally recognized investigations.

In addition to a broad array of cybersecurity and forensics experience, Jason is a noted instructor and speaker, teaching dozens of cybersecurity and forensics courses domestically and internationally to FBI staff, law enforcement agencies, and private sector partners. He has been an instructor at California State University Fullerton since 2008 and is a sought-after speaker at multiple industry events.

As an attorney, Jason has experience in complex business, real estate, and insurance law as well as commercial transactions. He served as legal clerk and intern for the Honorable D. Howell Jensen, U.S. District Court, and at the Santa Clara County District Attorney's Office.

Jason is the founding Laboratory Director of the Orange County Regional Computer Forensics, working to make that facility the largest of its kind in the nation, with 17 partner agencies and 30+ full-time laboratory personnel. He also expanded the mobile forensics program into one of the largest and most successful in the country.

Jason holds numerous certifications and memberships in the areas of global information security, computer forensics, laboratory management, and more. He has additional professional training, including 2,500 hours of Specialized Computer Forensics, Cyber, Management, and Laboratory Accreditation classes and instruction.

Areas of Focus

Services

- Information Privacy, Security and Governance
- Cybersecurity and Incident Response Services
- eDiscovery
- Information Governance
- Information Privacy
- Information Security

Credentials

Bar Admissions

- California

Education

- Santa Clara University School of Law, J.D., 1992, Associate Editor - *Santa Clara Law Review*
- University of California, Los Angeles, B.A., 1989, Honors; Chancellor's "Marshall Award" for Outstanding School Service and Achievement; Elected USAC Facilities