LAST-MINUTE
AMENDMENTS

Changes to California's New Privacy Law Ahead of the Effective Date

October 30, 2019

orrick

Introductions

Heather Sussman

Co-Chair
Cyber, Privacy & Data Innovation

hsussman@orrick.com

Emily Tabatabai

Partner
Cyber, Privacy & Data Innovation

etabatabai@orrick.com

@EmilyTabatabai

Nick Farnsworth

Associate
Cyber, Privacy & Data Innovation

nfarnsworth@orrick.com

Agenda

- Overview of the *Pre-Amendment* CCPA
- Successful CCPA Amendments
  - Personal Information & Privacy Notice Clarifications
  - Personnel Exception
  - Business-to-Business Exception
  - Data Broker Registration
  - Data Breach Personal Information
  - Consumer Rights and Exceptions Clarifications
- Bills Failing to Reach the Finish Line
- AG Regulations, CCPA 2.0 and Anticipating Next Year's Changes

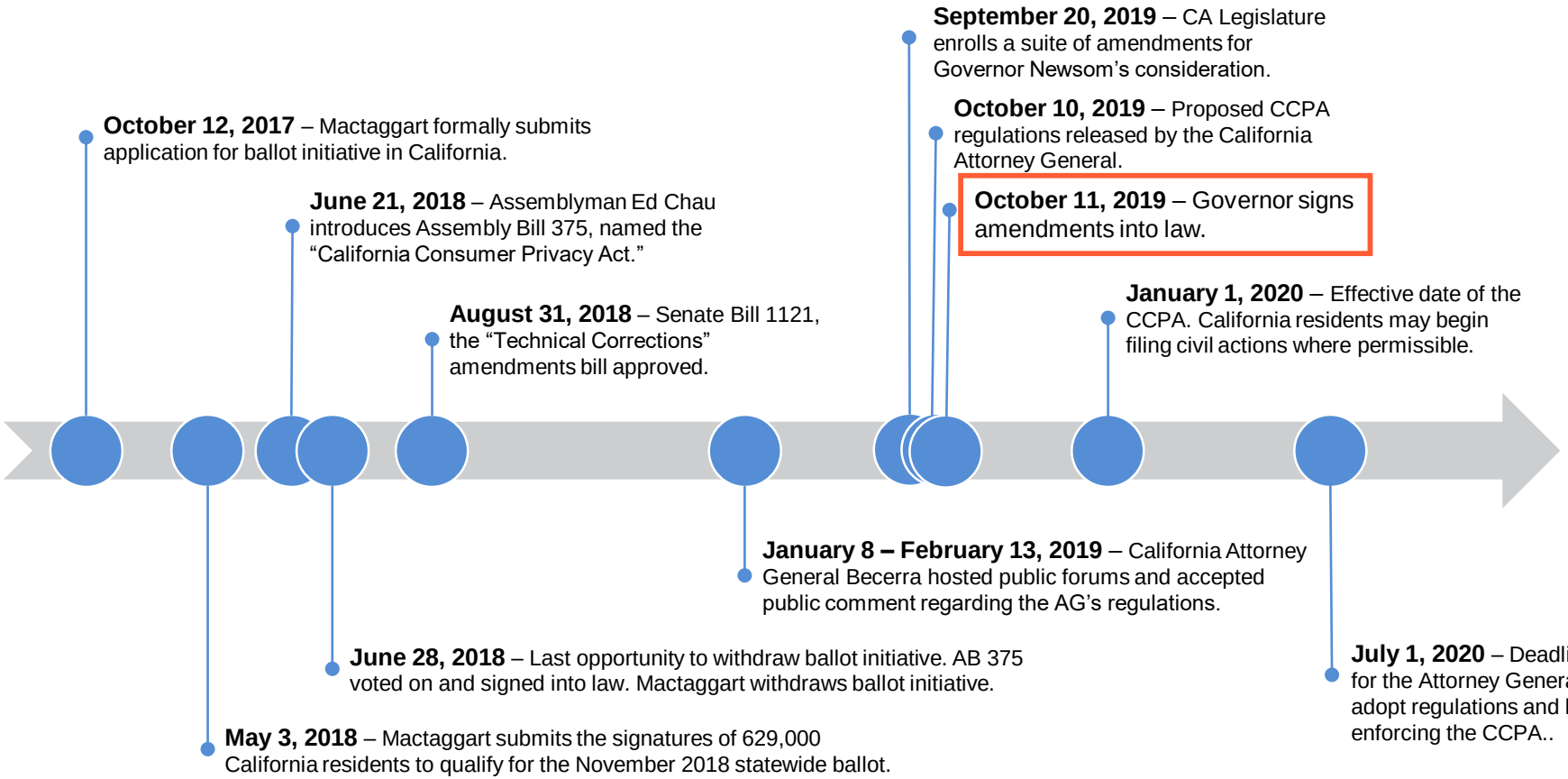
orrick

Overview
of the *Pre-Amendment* CCPA

orrick

The California Consumer Privacy Act (CCPA)

Effective January 1, 2020, the CCPA imports GDPR-style consumer rights around data ownership, transparency and control to the United States



CCPA: Applies to a "Business"

- **A Business:**
  - **For-profit** entity
  - Does business in California
  - Collects, receives or accesses California residents' personal information
  - Decides **why and how** such personal information is used or processed,

  AND

  - Satisfies at least one of the following criteria:
    - **Gross revenue over $25M** per year; **or**
    - Collects or shares the personal information of **>50,000 CA residents, households or devices** per year for a commercial purpose; **or**
    - Derives **50% or more of its revenue from selling CA residents'** personal information

Any entity that (i) controls or is controlled by and (ii) shares common branding with a "business" is also treated as a "business" under the law.

CCPA: Governs Use of "Personal Information"

Expansive Definition of "Personal Information" – Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular ***consumer*** or ***household.***

THE USUAL SUSPECTS

- Name
- SSN
- Financial Information *(exc. GLBA)*
- Contact Information
- Signature
- Physical Characteristics
- Insurance Policy Number
- Other Gov't IDs
- Health Data *(exc. HIPAA)*
- Passport
- Driver's License

PROTECTED CLASSIFICATIONS

- Race
- Citizenship
- Color
- National Origin
- Military Status
- Religion
- Gender Identity and Expression
- Sex
- Medical Condition or Disability
- Marital Status
- Age
- Genetic Information

BIOMETRIC AND GEOLOCATION INFORMATION

SENSORY DATA

- Audio
- Electronic
- Visual
- Thermal
- Olfactory
- Similar Information

BEHAVIORAL AND PROFILING DATA

- Tendencies
- Products/Services Considered
- Inferences
- Interest Data
- Order History
- Search History
- Purchase History

INTERNET OR OTHER ELECTRONIC NETWORK ACTIVITY

- Search History
- Browsing History
- Cookie Data
- IP Address
- Interest Data
- Online Interactions

PROFESSIONAL, EMPLOYMENT AND EDUCATION-RELATED INFORMATION

A consumer is a California resident . . . however identified, including by any unique identifier.

CCPA: Exemptions and Exceptions

Privacy Regime Exemptions

- Exempts personal information processed pursuant to federal or state privacy regimes:
  - the Gramm-Leach-Bliley Act (GLBA)
  - the California Financial Information Privacy Act (CFIPA)
  - the Driver's Privacy Protection Act (DPPA)
  - the Health Insurance Portability and Accountability Act (HIPAA)
  - the California Confidentiality of Medical Information Act (CMIA)
  - clinical trial information collected under the Common Rule
  - the Fair Credit Reporting Act (FCRA), broadened by recent amendment

Other Exceptions

- Exceptions for information maintained in a certain form or used in a certain way:
  - deidentified or aggregate information
  - wholly out-of-state commercial conduct information
  - to exercise or defend legal claims
  - to protect evidentiary privilege
  - to comply with laws, cooperate with law enforcement investigating unlawful activity, or comply with a government inquiry, investigation, subpoena or summons
  - to protect the rights and freedoms of other consumers

Under the CCPA, a "Business" must:

DISCLOSE online:

- categories of PI it collects, sells and otherwise discloses for a business purpose;
- categories of sources of the PI;
- business or commercial purposes for collecting or selling the PI; and
- description of the consumers' rights and the designated methods for submitting requests.

PROVIDE ACCESS:

- to the PI collected over the past 12 months in a ***portable*** format, in response to a "verifiable consumer request"

DELETE:

- PI upon a "verifiable consumer request" (and direct "service providers" to delete), subject to exceptions

PERMIT OPT-OUT:

- of data "sales" to third parties (including via "Do Not Sell My Personal Information" link), subject to exceptions

OBTAIN OPT-IN CONSENT:

- for children under 16, for "sales" of PI to a third party ("actual knowledge" and "willfully disregard" standard)

TRAIN EMPLOYEES:

- about the business' privacy practices, compliance and how to direct consumers to exercise their rights

NOT DISCRIMINATE:

- Against consumers who exercise their rights under the CCPA, **but** some financial incentives permissible ("Pay-for-Privacy")

CONTRACT *effectively:*

- *relative to "service providers" to establish scope of permissible data uses and mechanism for complying with consumer access/deletion requests*

Enforcement & Liabilities

AG Enforcement: Civil penalty of $2,500 (per violation) to $7,500 (per intentional violation) and injunctive relief.

- Enforcement is triggered upon violation(s) of CCPA.
- 30-day notice and cure period before AG may bring an enforcement action.

Limited Private Right of Action for Data Breach: Statutory damages not less than $100 and not greater than $750 "per consumer per incident," or actual damages (whichever is greater); injunctive or declaratory relief.

- Consumers may bring an action when certain personal information is subject to unauthorized access and exfiltration, theft or disclosure as a result of a failure to implement and maintain reasonable security measures.
- 30-day notice and cure period before filing.

Successful CCPA Amendments

Personal Information & Privacy Notice Clarifications

orrick

Personal Information & Privacy Notice Clarifications

"Personal Information" – Information that identifies, relates to, describes, is **reasonably** capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

- Does not include deidentified or aggregate consumer information.
- Does not include "publicly available" information regardless of purpose of use (removing the original compatibility requirement.

Amendments further clarify that there is no requirement:

- To collect/retain personal information not collected or retained in the ordinary course.
- To reidentify or link information that is not maintained as personal information.
- To disclose the actual specific pieces of personal information in the online privacy notice.

Successful CCPA Amendments

Personnel Exception

Personnel Exception Amendment (AB-25)

- Until January 1, 2021, the Personnel Exception applies to:
  - Personal information collected by a business about a natural person in the course of the natural person acting as a job applicant to, employee of, officer of, director of, medical staff member of, contractor of, or controlling owner of the business (collectively, "personnel") to the extent the personal information is collected and used by the business solely within the context of the natural person's current or former personnel role;
  - Personnel's emergency contact information; and
  - Personal information necessary to administer benefits for personnel's family members or other related persons.

Applies to all CCPA obligations other than a limited disclosure obligation and use limitation (Section 1798.100(b)) and the private right of action for certain breaches (Section 1798.150).

Personnel Exception Impact

- ☑ Specific Disclosures at Collection
- ☑ Civil Liability for Data Breach

- ☒ Rights to Know
- ☒ Right to Request Deletion
- ☒ Right to Opt Out of Data Sales
- ☒ Right to Non-Discrimination

Data Mapping	Personnel Notice	Reasonable Security
Personal information about personnel and related persons should be maintained in a business' **data map** or **personal information inventory**	A basic **Personnel Privacy Notice and Job Applicant Privacy Notice** should be drafted to address the CCPA's applicable disclosure obligations	Existing personnel information security measures/practices should be **assessed** **and** The **Incident Response Plan** should be **drafted or revised** to properly address personnel information, if necessary

*** Exception currently only applies until January 1, 2021.**

Successful CCPA Amendments

Business-to-Business Exception

orrick

Business-to-Business Exception Amendment (AB-1355)

- Until January 1, 2021, the Business-to-Business Exception applies to:
  - Personal information that reflects a communication or transaction between a business and the employees of a third-party entity (as well as the officers, directors, contractors and controlling owners of the third-party entity)
  - occurring solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such third-party entity.

Applies to all CCPA obligations other than the right to opt out or, for children, to opt in to "sales" (Section 1798.120), the right against discrimination (Section 1798.125) and the private right of action for certain breaches (Section 1798.150).

PRACTICE NOTE: It is not wholly clear which third-party entity representative personal information the B2B Exception will cover as information "reflect[ing] a communication or transaction." The statutory drafting leaves room for interpretation.

Business-to-Business Exception Impact

- ☑ Right to Opt Out of Data Sales
- ☑ Right to Non-Discrimination
- ☑ Civil Liability for Data Breach
- ☒ Specific Disclosures in Privacy Notice
- ☒ Rights to Know
- ☒ Right to Request Deletion

Data Mapping	Sale Analysis	Reasonable Security
Personal information about third-party entity representatives should be maintained in a business' **data map** or **personal information inventory**	Sharing of third-party entity personal information should be **monitored** to identify and remediate potential "sales," when possible Provide B2B consumers with the Right to Opt-Out of Sales	Existing personnel information security measures/practices should be **assessed** **and** The **Incident Response Plan** should be **drafted/revised** to properly address third-party entity representative information, if necessary

*** Exception currently only applies until January 1, 2021.**

Successful CCPA Amendments

Data Broker Registration

orrick

Data Broker Registration Requirement (AB-1202)

- The Data Broker Registration Requirement obligates businesses knowingly collecting and "selling" personal information, without a direct relationship with the relevant consumer, to:
  - register as a "data broker" with the California Attorney General; and
  - provide contact information to be made available on the Attorney General's website.

- A business is not a "data broker" to the extent that the business:
  - is subject to the Fair Credit Reporting Act, Gramm-Leach-Bliley Act or Insurance Information Privacy Protection Act; or
  - has a direct relationship with the consumer whose personal information it "sells."

PRACTICE NOTE: The Data Broker Registration Requirement does not directly amend the CCPA, but instead adds an act to a separate title just prior to the CCPA in the California Civil Code. Businesses that "sell" personal information will need to determine whether registration with the California Attorney General is required. If required, registration will permit consumers to locate a business's website that they may otherwise have been unaware of and opt out of "sales."

Successful CCPA Amendments

Data Breach Personal Information

orrick

Data Breach Notification Statute Revisions – AB-1130

- Though not technically part of the CCPA, the CCPA's private right of action provision (1798.150) incorporates the CA Customer Records statute by reference.
- Customer Records statute (1798.81.5) defines "Personal Information" to mean:
  - SSN, Driver's license number, CA ID number, tax ID number, passport number, military ID number, or other unique government-issued ID number;
  - Account number of credit or debit card, in combination with security code or password that would permit access to a financial account;
  - Medical information, health insurance information;
  - Unique biometric identifier generated from human body characteristics, such as fingerprint, retina or iris image, used to authenticate an individual, and a physical or digital photograph *if* used for facial recognition purposes; or
  - A user name or email address and password that permits access to an online account.

Successful CCPA Amendments

Consumer Rights and Exceptions Clarifications

orrick

Consumers Rights & Exceptions Clarifications

Consumer Rights: Clarifies the business's consumer rights obligations by .

- Replacing **toll-free number requirement with email address requirement** for businesses operating exclusively online and having direct relationships with consumers.
- Requiring businesses with **internet websites** to make them available for requests.
- Permitting business to require requests **through account** where an account is maintained.
- Adds deletion exception to fulfill terms of **written warranty** or **product recall**.
- Adds opt-out exception for motor vehicle dealer/manufacturer sharing for **warranty/recall**.
- Clarifies discrimination does not occur where difference in price, rate, level or quality is reasonably related to the value provided to the **business** by the consumer's PI.

CCPA Exception: Broadens FCRA exception to exclude (other than private right of action) processing or selling of PI by an agency, furnisher, or user subject to FCRA.

Failed CCPA Amendments

orrick

Failed CCPA Amendments

The following bills failed to pass the California legislature and will not become law this year:

General Private Right of Action

Private right of action for *any* CCPA violation, as well as eliminated right to seek individualized guidance from AG and to cure an alleged CCPA violation within 30 days to avoid enforcement action

Loyalty Programs

Clarified nondiscrimination right does not prohibit voluntary loyalty or rewards program, but prohibited "sale" of PI in connection with such programs except in limited circumstances

Targeted Advertising "Do Not Sell" Exception

Account Closure

Required social networks to provide option to delete and prohibit sale after account is closed

Social Media

Prohibited social media service from allowing children under 13 years of age to create an account without parental or guardian consent

Additional Disclosures*

Required disclosure of monetary value of data and the use of facial recognition

Affirmative Opt-In Consent for Sharing of Personal Information*

These bills could be reintroduced in some form for reconsideration next year

What's Next?

Additional Changes in Law

AG Regulations

Proposed CCPA regulations were released October 10, 2019 with final regs potentially by January 1, 2020 addressing:

- Notice to Consumers
- Business Practices for Handling Consumer Requests
- Verification of Requests
- Special Rules Regarding Minors
- Nondiscrimination

CCPA 2.0

Alastair Mactaggart, a driving force behind the CCPA, recently unveiled a 2020 ballot initiative that would:

- Create the California Privacy Protection Agency
- Add sensitive personal information requirements
- Introduce Right to Correct
- Bolster children's privacy protections
- Increase disclosure obligations

Federal & State Laws

Congress continues to consider a **comprehensive federal privacy law** with support from many industry lobbyists that could preempt state laws

and

Over 15 states considered **CCPA-like comprehensive privacy statutes**, which will likely be reconsidered next year

What Should Companies Do to Prepare?

- **Develop complete and accurate data maps of all information identifying or relating to an individual (regardless of residency).**
- **Be prepared to receive and respond to consumer requests promptly and to maintain records off the business's consumer request practices.**
- **Build flexibility into CCPA compliance programs, such as by building overarching frameworks and protocols that can adapt as laws change.**
- **Stay up-to-date on the latest privacy developments (you can signup for client alerts by emailing qlin@orrick.com).**

QUESTIONS?

orrick

Orrick's Privacy Law Webinar Series
Part #6: CCPA Compliance – It's Not Too Late to Get Started

Webinar | November 21 | 12pm – 1pm (Eastern Standard Time)

California has introduced sweeping changes in the U.S. privacy landscape. Starting January 1, 2020, the new privacy law will affect most medium to large businesses located in California, or doing business in California, regardless of where the business is located. Are you prepared?

This webinar is the sixth in a series on U.S. privacy law developments in 2019.

Presenters

Heather Sussman, Partner

Kyle Kessler, Managing Associate

Orrick's Privacy Law Webinar Series

- ✓ Want to learn about the new U.S. privacy laws and the impact they may have on your business?
- ✓ Missed a past webinar?
- ✓ Want to attend our next webinar?
- ✓ Visit **https://www.orrick.com/Cyber-Privacy-Webinars-Videos**

California was the first U.S. state to enact a sweeping new privacy law, the CCPA, which comes into effect in January 2020. Nevada has now enacted a scaled-down version of the CCPA that is now effective.

Orrick's CCPA & GDPR Readiness Assessment Tools

Orrick's ccpa READINESS ASSESSMENT

Test your company against the provisions under the CCPA

- Receive a complimentary report summarizing the likely key impacts
- Use the report to develop your CCPA project plan

Visit: orrick.com/Practices/CCPA-Readiness

Orrick's GDPR Readiness Assessment Tool

Stress test your company against the provisions under the GDPR

- Receive a complimentary report summarizing the likely key impacts
- Use the report to develop your GDPR project plan

Visit: orrick.com/Practices/GDPR-Readiness

Trust Anchor

An established point of trust in a cryptographic system from which a process of validation can begin

Blog: blogs.orrick.com/trustanchor
Twitter: @Trust_Anchor

Heather Egan Sussman

Partner
Boston

T 617 880 1830
E hsussman@orrick.com

Honors

- *Chambers USA* 2019
- *The Legal 500 United States* 2019
- *Cybersecurity Docket's* "Incident Response 30" 2016, 2018, 2019
- *Massachusetts Lawyers Weekly* "Top Women of Law" 2015
- *Best Lawyers* 2018-2019

Education

- J.D., Boston College Law School, 2000
- B.A., University of Massachusetts Dartmouth, 1996, *magna cum laude*

Heather Egan Sussman is Global Co-chair of Orrick's Cyber, Privacy & Data Innovation practice and the leader of Orrick's Boston Office. Her practice focuses on privacy, cybersecurity and information management, and she is ranked by *Chambers USA* and *The Legal 500 United States* as a leader in her field. *Chambers* explains companies turn to Heather because she is "generous with her time and endeavors greatly to educate her clients and understand a given client's risk profile."

Heather's practice focuses on privacy, cybersecurity and information management. Heather routinely guides clients through the existing patchwork of laws impacting privacy and cybersecurity around the globe. In the United States this includes advising on federal and state laws such as CCPA, FCRA, ECPA, TCPA, HIPAA, CAN-SPAM, GLBA, state breach-notification laws, and state data-security laws, as well as existing self-regulatory frameworks, including those covering online advertising and payment-card processing. Outside of the United States, she manages teams of talented counsel around the world to deliver seamless advice for clients that operate across many jurisdictional lines, developing comprehensive privacy and cybersecurity programs that address competing regulatory regimes. Heather drafts online privacy notices for global rollout and implements data-transfer mechanisms for the free flow of data worldwide. She helps clients develop and achieve their data innovation strategies, so they can leverage the incredible value of data and digital technologies in ways that not only meet compliance obligations but also support innovation, deliver value to the business, meet security needs and solidify brand and consumer trust. Heather helps clients reduce the risk of privacy and security incidents and, in the event of a privacy or security breach, she helps companies respond. She guides clients through comprehensive privacy and cybersecurity assessments worldwide. Heather also regularly counsels businesses on how to mitigate risks associated personal data.

Emily S. Tabatabai

Partner
Washington, D.C., Houston

T 202 339 8698
E etabatabai@orrick.com
@EmilyTabatabai

Honors

- *Chambers USA* - Nationwide, Privacy & Data Security, Up and Coming attorney (2018-2019)
- *The Legal 500,* Cyber Law - Including Data Protection and Privacy (2017-2019)
- Member of IAPP Publications Advisory Board (2019)
- Member of Law360 Privacy Editorial Advisory Board (2018)
- *Law360,* Privacy Practice Group of the Year (2016)
- *The Legal 500*, Media Technology and Telecoms, Cybercrime (2014-2016)

Education

- University of Virginia School of Law, J.D., 2006
- Emory University, Goizueta Business School, B.B.A., 2001

Emily S. Tabatabai is a partner and founding member of the Cyber, Privacy & Data Innovation practice, which was named the Privacy & Data Security Law Firm of the Year by Chambers USA in 2019. She has been recognized by *The Legal 500* for her "extraordinary depth of knowledge in student data privacy matters," and by *Chambers USA* as "an invaluable resource to have when it comes to data privacy and security...on the student data side, she is unmatched."

Emily advises clients on an array of privacy and data-management matters, helping clients navigate the complex web of privacy laws, rules, regulations and best practices governing the collection, use, transfer and disclosure of data and personal information. She works closely with client business teams and in-house counsel to assess and manage privacy risks, design and deploy compliance programs and implement privacy-by-design approaches to address key compliance objectives while supporting each client's data innovation strategies and the development and use of cutting-edge digital technologies.

Emily frequently guides child- and student-directed service providers through the complexities of compliance with the Children's Online Privacy Protection Act (COPPA), the Family Educational Rights and Privacy Act (FERPA), California's Student Online Personal Information Protection Act (SOPIPA) and similar state student-privacy laws and advises companies across the industry spectrum as they work towards compliance with the California Consumer Privacy Act (CCPA). She also represents clients subject to regulatory investigations and litigation involving a spectrum of federal and state laws, including under Section 5 of the Federal Trade Commission Act (FTC Act), COPPA, the Fair Credit Reporting Act (FCRA), Gramm-Leach-Bliley Act (GLBA), the U.S.-E.U. Privacy Shield Program, the California Online Privacy Protection Act (CalOPPA) and others.

Nicholas Farnsworth

Associate
Boston

T 617 880 1855
E nfarnsworth@orrick.com

Education

- Georgetown University Law Center, J.D., 2017, *Magna Cum Laude*; Order of the Coif; Executive Editor, *The Georgetown Law Journal*
- Harvard College, A.B., Economics, 2012

Privacy and cybersecurity underpins the innovative strategies of businesses across all sectors and introduces both legal and operational concerns. As a member of Orrick's internationally recognized Cyber, Privacy & Data Innovation team, Nick Farnsworth advises clients on a broad range of privacy and cybersecurity matters, including compliance, risk management and incident response.

Nick's practice focuses on guiding clients through the existing patchwork of state, federal and international privacy and cybersecurity laws. His practice includes advising clients on Section 5 of the Federal Trade Commission Act, the Fair Credit Reporting Act (FCRA), the Telephone Consumer Protection Act (TCPA), CAN-SPAM, state breach-notification laws and state privacy and cybersecurity laws, such as the California Consumer Privacy Act (CCPA). Nick also advises clients on the impact of international laws from a U.S. perspective, including the European Union General Data Protection Regulation (GDPR).

Nick assists clients from a broad range of industries and sectors in assessing their current privacy and cybersecurity practices. He regularly assists clients in developing global privacy and cybersecurity programs to practically implement the principles and obligations underlying various legal regimes, as well as assessing proposed marketing/advertising, transactional and business strategies from a privacy and cybersecurity perspective. Nick also advises clients on the assessment of suspected incidents/breaches and any associated notification obligations, as well as the privacy and cybersecurity risks associated with proposed transactions and ventures.

In addition, Nick has an active pro bono practice, which has included representing clients in immigration and innocence matters and assisting small businesses with their legal needs.

To make the California Consumer Privacy Act more accessible, Nick was a member of the team that developed Orrick's CCPA Readiness Assessment Tool. The tool provides companies an opportunity to test their preparedness for compliance with the CCPA as a first step to constructing their strategic compliance roadmap.

orrick