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.

Drinker Biddle®

INFORMATION PRIVACY, SECURITY AND GOVERNANCE

IPSG: How Can We Help?

Organizations and companies across all industries collect, use and store ever increasing amounts of data in the course of day-to-day operations, which raises privacy, security, information management, e-discovery, and other legal compliance issues. Our Information Privacy, Security and Governance (IPSG) team brings together lawyers and professionals across multiple areas of the firm to assist clients with assessing information privacy and security practices, developing information governance programs, responding to regulatory compliance inquiries and investigations, and handling litigation related to information privacy and security compliance.

MISSION

Our mission is to assist clients in maximizing the value of their data assets while minimizing regulatory and legal risks and safeguarding the data from security vulnerabilities.

Scalable Assessments

We evaluate an organization's overall compliance, or particular compliance of a data processing activity or technology, with IPSG requirements and best practices.

Data Mapping

Map an organization's databases and/or data processing activities through questionnaires and interviews, or with the assistance of automated tools.

Gap Analysis

Compare the privacy and security practices and controls in place to legal requirements, industry standards, and best practices.

Vulnerability Testing

Use trusted vendors to assist with testing of security controls.

Training

We train employees, executive management, and boards on IPSG topics.

Live Instruction

Conduct in-person, interactive training at organizational events.

Software Modules

Develop content for training modules and work with Drinker Biddle or client's own training vendor to automate training.

Tabletop Exercises

Develop simulated exercises (e.g., security incident) to review and discuss actions that should be taken and clarify organizational roles and responsibilities.

Tool Box for Client's IPSG Program

We develop policies, procedures, contract language, forms, checklists, and other job-aids to assist organizations in managing their IPSG functions.

Policies and Procedures

Develop new or revise existing policies and procedures covering a wide range of privacy, security, and information governance issues.

Contracting Playbook

Incorporate template privacy and security language in contracts with vendors and other third parties, as well as provide guidance for contracting personnel on how to respond to likely pushback.

Job Aids

Develop guides, checklists, forms, and other job aids for use by employees to ensure that they are adhering to privacy, security, and information governance requirements, as well as for use by those in compliance and legal departments with responsibility for oversight.

Third-Party Assessment Guides

Develop questionnaires and guides for use in assessing the privacy, security, and information governance practices of prospective vendors, business partners, and acquisition targets.

Virtual Privacy Officer

We provide ongoing privacy compliance support to supplement an existing privacy program. Our team is also equipped to provide day-to-day privacy compliance support for organizations that do not have a dedicated privacy function or need to fill a temporary gap.

Data Strategy and Analytics

We counsel clients on structuring databases and data flows, and analyze data to uncover insights and in support of legal functions.

Data Strategy Counseling

Advise clients on how to structure their data processing activities in order to minimize legal barriers and maximize data value.

Analytics

Apply data analytics to aid in internal investigations, due diligence, data loss prevention, data remediation, auto-classification, and other compliance tasks.

Incident Response

We assess legal responsibilities in the event of a privacy or security incident and assist clients in managing their response, including communicating with government authorities and affected data subjects.

Incident Assessment

Evaluate the risks to the organization, data subjects, and third parties from incidents involving the potential loss, theft, or unauthorized access, use, or disclosure of informational assets.

Communications

Prepare communications to law enforcement, regulatory authorities and data subjects in accordance with legal requirements and organization's policies. Work with client's public relations team to respond to media inquiries.

Investigations and Litigation

We defend organizations in government investigations and prosecutions, as well as in individual and putative class actions, for alleged non-compliance with IPSG requirements.

Government Actions

Assist in management of client communications with and representation before regulatory authorities. Work with client to investigate facts and prepare defenses.

Private Litigation

Defend clients in individual and putative class actions in courts across the country.

Information Privacy, Security and Governance Group

Reed Abrahamson
Associate | Washington, D.C.
(202) 230-5672
Reed.Abrahamson@dbr.com

Peter A. Blenkinsop
Partner | Washington, D.C.
(202) 230-5142
Peter.Blenkinsop@dbr.com

Jeremiah Posedel
Associate | Chicago
(312) 569-1504
Jeremiah.Posedel@dbr.com

Drinker Biddle®

www.drinkerbiddle.com

CALIFORNIA | DELAWARE | ILLINOIS | NEW JERSEY | NEW YORK | PENNSYLVANIA | TEXAS | WASHINGTON DC | LONDON

Presenters:
Jeremiah Posedel
jeremiah.posedel@dbr.com

Justin O. Kay
justin.kay@dbr.com

Amy E. Keller
akeller@dicellolevitt.com

California Consumer Privacy Act

CCPA Webinar #3

Litigation Risk, Defenses, and Damages

May 8, 2019

Drinker Biddle

Agenda

I. Overview of CCPA
II. AG Enforcement
III. Private Right of Action
IV. Proposed Amendments
V. Webinar Series Schedule
VI. Questions

CCPA Overview

Consumer Rights

- The right to know what **personal information** is being collected about them.
- The right to know whether their personal information is sold or disclosed and to whom.
- The right to say no to the sale of personal information.
- The right to access and delete their personal information.
- The right to equal service and price, even if they exercise their privacy rights.

The Scope of the CCPA

- The CCPA applies to **personal information** about California **consumers** or households.
- The CCPA applies to any for-profit **business** that does business in California with any of these qualities:
  - Has annual gross revenues greater than $25 million,
  - Annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes **personal information** about more than 50,000 **consumers**, households, or **devices,** or
  - Derives 50% or more of its annual revenues from **selling consumer's personal information**.

The Scope of the CCPA

- **"Personal Information"**
  - Any information 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."
- **"Selling"** personal information
  - "Selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration."
  - Certain activities excluded from scope/meaning of "sale".

Californians' Rights - Transparency

- **Right to Notice at Collection**: A business has to provide notice at or before the point of collection about the categories of information to be collected and the purposes for which the personal information will be used.
- **Right to Request Information**: In response to a "verifiable consumer request," a business must disclose:
  - the categories of personal information the business has collected about that consumer,
  - the specific pieces of personal information it has collected about that consumer,
  - the categories of sources from which the personal information is collected,
  - the categories of third parties with whom the business shares personal information,
  - the categories of personal information that the business has sold about the consumer, by category or categories of personal information for each third party to whom the personal information was sold, and
  - the business or commercial purpose for collecting or selling personal information.

Categories of Personal Information

- Identifiers such as:
  - Name
  - Alias
  - Postal address
  - Email address
  - Online identifier
  - IP address
  - SSN
  - Driver's license number
  - Passport number
- Characteristics of protected classifications under California or federal law.
- Biometric information.
- Geolocation data.
- Audio, electronic, visual, thermal, olfactory, or similar information.
- Professional or employment-related information.
- Education information.
- Commercial information, including records of purchasing or consuming histories.
- Internet or other electronic network activity information, such as browsing and search history.
- Inferences used to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, or aptitudes.

Business's Obligations – Website Notice

- **Website Notice Requirements:** A business must disclose, on its website and in other public notices directed at California consumers:
  - The **categories of personal information** that it has collected about consumers in the preceding 12 months and the **purposes** for the collection,
  - The **categories of sources** from which the personal information was collected,
  - The **categories of third parties** with whom the business shares personal information,
  - The **categories of personal information about consumers that it has disclosed for a business purposes** in the preceding 12 months, and
  - The **categories of personal information about consumers that it has sold** in the preceding 12 months and the **purposes** of the sale OR a statement that the business has not sold any consumers' personal information in the preceding 12 months

Californians' Rights – Access and Deletion

- **Right of Access**: In response to a verifiable consumer request, a business must disclose, free of charge, the personal information it has collected about that consumer. If delivered electronically, the information must be in a portable format, to the extent technically feasible.
  - Like the "Right to Portability" under the GDPR.
- **Right to Request Deletion:** In response to a verifiable consumer request, a business must delete personal information which the business has collected from the consumer.
  - A business may decline to delete data if it meets a particular exemption for internal use or use in relation to its relationship with the consumer.

Californians' Rights – Opt-Out of Sale

- **Right to Opt-Out:** A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third-parties not to sell the consumer's personal information.
- **No Sale of Personal Information of Minors Without Opt-In:** A business may not sell personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age without the minor's consent (if over 13) or the parent/guardian's consent (if under 13).
  - Willful disregard of a consumer's age shall be deemed actual knowledge.

Business's Obligations – Opt-Out Mechanism

- **"Do Not Sell" Button:** A business that sells personal information must provide a clear and conspicuous link on the business's homepage, titled "Do Not Sell My Personal Information," to a web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal information.

Do Not Sell My Personal Information

Business's Obligations – Prohibition on Discrimination

- **Non-discrimination**: A business may not charge consumers more or offer reduced services if the consumer exercises their rights. However, a business may offer certain financial incentives to consumers or adjust pricing or service levels based on the value of the consumer's data to the consumer.

Business's Obligations – Prohibition on Waiver

- **No Waiver**: Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under the CCPA, including, but not limited to, any right to a remedy or means of enforcement, will be considered contrary to public policy and shall be void and unenforceable.

Exemptions

- The obligations imposed by the CCPA shall not restrict a business's ability to:
  - comply with federal, state, and local law,
  - comply with civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by a federal, state, or local authority,
  - cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law,
  - exercise or defend legal claims, and
  - claim evidentiary privileges or make communications that would be subject to evidentiary privileges.

Exemptions

- The obligations imposed by the CCPA do not apply to the collection, use, sale, retention, or disclosure of consumer information that is **deidentified** or in the **aggregate consumer information.**
- The obligations imposed by the CCPA do not apply to the **collection** or **sale** of a consumer's personal information if every aspect of the commercial conduct takes place wholly outside of California.
- **Other Laws:** The CCPA doesn't, *generally*, apply to information subject to the GLBA, California Financial Privacy Act, and Driver's Privacy Protection Act, or to consumer reports subject to the FCRA.

Cal AG Rulemaking

- AG required to issue rules before July 1, 2020 on following topics:
  - Are additional categories of personal information needed?
  - Does the definition of "unique identifiers" need to be updated?
  - What additional exceptions are needed to comply with state or federal law?
  - What rules and procedures should be established for submitting and complying with consumer requests?
  - What uniform opt-out logo/button would best promote consumer awareness?
  - What types of information or language are sufficient to provide consumers with easily understandable and accessible notice of their rights?
  - How should businesses verify and authenticate consumer requests?
- AG conducted public forums for interested persons to provide testimony.
- Formal rulemaking process will also allow opportunity for public comment.

AG Enforcement

AG Enforcement [§1798.155]

- The Attorney General may bring a civil action against any business, service provider, or other person who violates the Act.
- 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.
- No AG enforcement until 6 months after final regulations are published or July 1, 2020, whichever is sooner. [§1798.185]
- A business or third party may seek the opinion of the AG for guidance on how to comply with the Act.

AG Enforcement: Penalties

- The Attorney General may seek an injunction +
- Each violation may result in a civil penalty **≤ $2,500**
- Each intentional violation may result in a civil penalty of **≤ $7,500**
  - 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 AG.
  - Any civil penalty assessed shall be deposited in the Consumer Privacy Fund to offset any costs incurred by the state courts and the AG in connection with the Act.

Private Right of Action

Private Actions [§1798.150]

- Narrow Private Right of Action for data breaches involving *certain categories personal information*:

"Any consumer whose nonencrypted or nonredacted ***personal information*** *… is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information…"*

Private Actions: "Personal Information"

- PRA applies to breaches of "personal information" as defined under CA's general data security statute (Cal.Civ.Code § 1798.81.5).
- Narrow definition of "personal information" (compared to CCPA definition):
  - *An individual's first name or first initial and last name in combination with any one or more of the following: Social security number; 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.*
  - *A username or email address in combination with a password or security question and answer that would permit access to an online account.*

Private Actions: Relief

- Impacted consumers may bring a civil action for any of the following:
  - Damages
    - **Statutory damages** ≥ $100 and ≤ $750 (per consumer per incident) *or*
    - **Actual damages** (if greater than statutory damage amount)
  - Injunctive or declaratory relief
  - Any other relief the court deems proper
- Actions for statutory damages may be brought on an individual or class-wide basis.
- Private Actions available January 1, 2020 (*likely prior to AG ability to enforce*).
- The private right of action for data breaches specifically does apply when information is covered by the GLBA, Cal. Financial Privacy Act, and DPPA.

Private Actions: Relief

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

Private Actions: Prior Notice

- Before bringing an action for statutory damages, a consumer must provide the business with 30 days written notice of the violation, identifying the "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 Act that postdates the written statement.
- A consumer is not required to provide notice if seeking **actual damages**.

Proposed Amendments (*Impacting Enforcement*)

SB-561

1. Expands the private right of action to **any violations of the CCPA**.
2. Eliminates the requirement for the AG to provide a 30-day notice and cure period before bringing an enforcement action.
   - It would leave intact the 30-day notice and cure period with respect to private actions.
3. Specifies that the AG may publish materials that provide businesses with general guidance on how to comply with the Act (*instead of allowing a business to seek specific compliance guidance from the AG*).

SB-561 (cont.)

- Introduced by Sen. Hannah-Beth Jackson on Feb 22, 2019, after consultation with the AG's office.
  - AG's position is that private rights of action are a "critical adjunct" to the AG's ability to enforce.
- In April, CA Senate Judiciary Committee and Senate Appropriations Committee approved the bill.
  - Placed on Suspense File, where the committee sends bills with an annual cost of more than $150,000, to be considered following budget discussions. The bill will not move forward until the Appropriations Committee releases it for a vote.
  - Bill will likely undergo further revision.
- Key concerns raised during open hearing on SB-561:

Webinar Schedule

Webinar Schedule

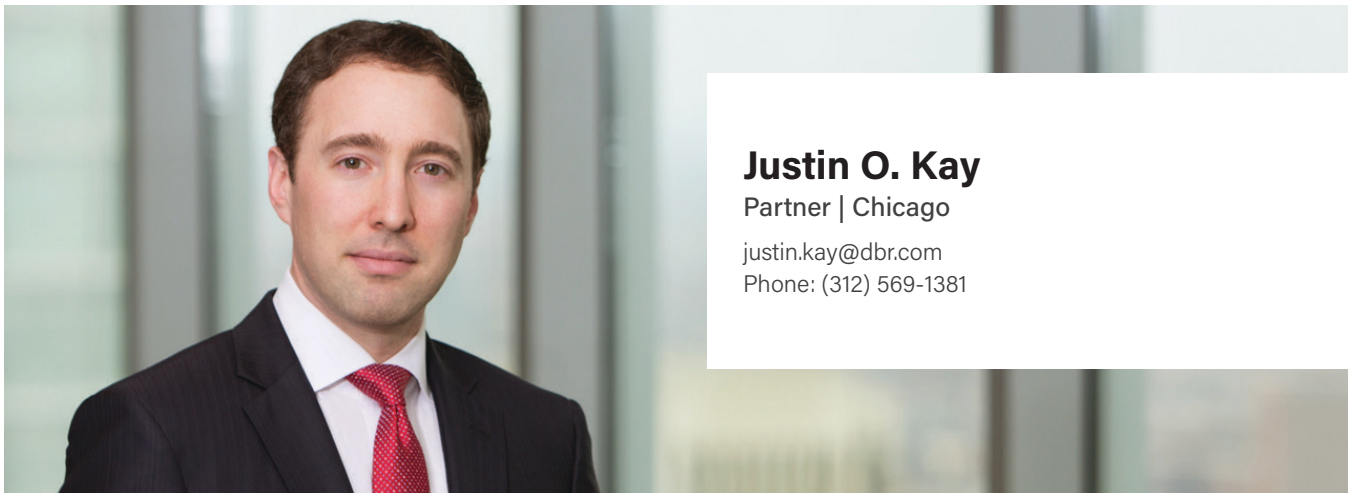
1:00 – 2:00 PM US Eastern

- Today
- June 12, 2019
- July 17, 2019
- August 21, 2019
- September 25, 2019
- October 30, 2019
- December 4, 2019

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

Questions

DrinkerBiddle®



Justin O. Kay

Partner | Chicago

justin.kay@dbr.com
Phone: (312) 569-1381

About

Justin O. Kay focuses on defending complex civil matters in federal court, state court, and before federal agencies. He is a regular contributor to the TCPA blog, a defense-oriented resource analyzing TCPA-related litigation and regulatory developments. Justin is a vice chair of the firm's Class Actions Team, a member of the TCPA Team, and chair of the firm-wide National Hiring Committee, which oversees the recruiting and hiring of associates.

Prior to his legal career, Justin served as an Intelligence Officer for the Department of Defense's National Geospatial Intelligence Agency.

Areas of Focus

Services

- Antitrust
- Appellate
- Class Actions
- Commercial Litigation
- Consumer Contracts
- Litigation
- Trade Secrets
- Securities and Corporate Governance Litigation
- Telephone Consumer Protection Act

Credentials

Bar Admissions

- District of Columbia
- Illinois

Court Admissions

- U.S. Court of Appeals, District of Columbia Circuit
- U.S. Court of Appeals, Seventh Circuit
- U.S. District Court, District of Columbia
- U.S. District Court, Northern District of Florida
- U.S. District Court, Northern District of Illinois
- U.S. District Court, Eastern District of Michigan
- U.S. District Court, Eastern District of Wisconsin

Education

- University of Notre Dame Law School, J.D., 2005, *cum laude*
- Georgetown University, B.S.F.S., 2000

Organizations

- Chicago Inn of Court
- BBVA Compass Chicago Advisory Director Board

DrinkerBiddle®

Jeremiah Posedel

Associate | Chicago

jeremiah.posedel@dbr.com
Phone: (312) 569-1504

About

Jeremiah Posedel is a member of Drinker Biddle's Information Privacy, Security and Governance team and Information Technology and Outsourcing team. Jeremiah's practice is at the interface of law, technology and privacy, integrating two distinct but overlapping domains: information technology transactions and data privacy and security.

First, Jeremiah advises on and negotiates a wide array of transactions involving the acquisition, development, leveraging and marketing of information technology assets, including hardware, software and database licensing, outsourcing and cloud-based services arrangements, and system implementation and support agreements.

Second, Jeremiah counsels clients on domestic and international privacy and security regulations and standards applicable to the collection, use and disclosure of personal data, including the FTC Act, GLBA, FCRA, HIPAA, COPPA, CAN-SPAM, TCPA, California Consumer Privacy Act (CCPA), NAIC model regulations and guidance, PCI DSS, DAA Program for Online Behavioral Advertising, and EU General Data Protection Regulation. He works with organizations to develop and implement comprehensive privacy/security programs and compliance strategies focused on a variety of data processing activities, including digital and interest-based advertising, big data analytics and profiling, blockchain deployment, workplace monitoring, mobile device and app deployment, cross-border data transfers, and InsurTech and e-commerce initiatives.

Jeremiah is a Certified Information Privacy Professional (US/Europe/Canada) and a visiting Lecturer of Law (information privacy) at Bucerius Law School in Hamburg, Germany. In 2004, Jeremiah served as a deputy campaign director to President Barack Obama's successful U.S. Senate campaign.

Areas of Focus

Services

- Information Technology and Outsourcing
- Intellectual Property
- International
- Technology Transactions and Licensing
- Information Privacy
- Information Security

Industries

- Health Care
- Pharma and Life Sciences
- Retail
- Insurance
- InsurTech
- Technology

Credentials

Bar Admissions

- Illinois

Court Admissions

- U.S. District Court, Central District of Illinois
- U.S. District Court, Northern District of Illinois

Education

- University of Illinois College of Law, J.D., 2006, *cum laude*
- Bucerius Law School, Hamburg Germany, 2006
- Valparaiso University, B.A., 2000, *cum laude*

Amy E. Keller
Partner

EMAIL:
akeller@dicellolevitt.com

EDUCATION
John Marshall Law School, J.D.

University of Michigan, B.A.

Amy Keller has built a national reputation as a zealous consumer advocate, directing litigation strategy in nationwide class action cases.

Amy Keller has experience successfully litigating a variety of complex litigation cases in leadership positions across the United States. As the Firm's Technology Practice Chair, Ms. Keller is the youngest woman ever appointed to serve as co-lead class counsel in a nationwide class action. Ms. Keller is currently leading two of the largest data breach cases in the country. In the nationwide litigation pending against Equifax related to its 2017 data breach, Ms. Keller represents nearly 150 million class members. *In re Equifax, Inc. Customer Data Security Breach Litig.*, No. 17-md-02800 (N.D. Ga.). In another case, against Marriott, Ms. Keller represents nearly 400 million consumers. *In re Marriott International, Inc. Customer Data Security Breach Litig.*, No. 19-md-02879 (D. Md.). As the Co-Chair of Law and Briefing on the Plaintiffs' Executive Committee in *In re Apple Inc. Device Performance Litig.*, No. 18-md-02827 (N.D. Cal.), Ms. Keller employed her technical savviness in directing an effort to craft a nationwide and international consolidated complaint. Ms. Keller's numerous other leadership positions have also required sophistication in not only understanding complex legal theories, but also presenting multifaceted strategies to ensure a favorable result to her clients. *See, e.g., Gengler v. Windsor Window Company, et al.*, No. 16-cv-00180 (E.D. Wis.) (plaintiffs' steering committee; case resulted in nationwide settlement); *Catalano v. BMW of North America, LLC, et al.*, No. 15-cv-04889 (S.D.N.Y.) (interim settlement counsel for nationwide settlement providing repair and replacement of certain electrical parts in automobiles); *Roberts, et al. v. Electrolux Home Prods., Inc.,* No. 12-cv-01644 (C.D. Cal.) (co-lead settlement counsel in nationwide, $35 million settlement).

Ms. Keller's expertise spans a wide variety of practice areas and topics—including consumer protection, breach of warranty, product liability, financial fraud, and employment litigation. Ms. Keller's experience also extends to the development of briefing and strategy at the district and appellate court level concerning ascertainability of class members in consumer class actions, complex personal jurisdiction challenges in multi-state cases, the use of conjoint analysis in determining damages, and the enforceability of arbitration clauses in consumer contracts. See, e.g., *Conagra Brands, Inc. v. Briseño, et al.*, 138 S. Ct. 313 (2017); *Bell v. PNC Bank, Nat. Ass'n*, 800 F.3d 360 (7th Cir. 2015); and *Sloan v. General Motors LLC*, 27 F. Supp. 3d 840 (N.D. Cal. 2018), among others.

As a two-time chair of the Chicago Bar Association Class Action Committee, Ms. Keller gave a number of presentations on topics impacting large-scale consumer class actions, including presentations on emerging legal issues in technology matters, such as Article III standing in privacy and data breach cases. Ms. Keller is recognized by Illinois Super Lawyers as a "Rising Star," and serves as a board member of Public Justice, a not-for-profit legal advocacy organization. She is a member of the Sedona Conference's Working Group 11, which focuses on litigation issues surrounding technology, privacy, artificial intelligence, and data security, and is also on the Model Data Breach Notification Principles drafting team. She also serves on the Cybersecurity & Privacy Editorial Advisory Board for *Law360*, where she brings plaintiffs' counsel's perspective to the publication's analysis of data breach cases. In 2018, Ms. Keller was named a *National Law Journal* Plaintiff Trailblazer, and one of the "Top 40 Under 40" trial lawyers in Illinois by National Trial Lawyers. She is also on the production team, writer, and a dancer for the Chicago Bar Association's annual Bar Show, now in its 97th year.