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

California Consumer Privacy Act

Presenters:

Peter Blenkinsop
peter.blenkinsop@dbr.com

Reed Abrahamson
reed.abrahamson@dbr.com

Jeremiah Posedel
jeremiah.posedel@dbr.com

CCPA Webinar #1
February 27, 2019

Drinker Biddle

Agenda

I. Overview of Webinar Series
II. Introduction to CCPA
III. What to Expect in 2019
IV. Questions

Webinar Schedule

1:00 – 2:00 PM US Eastern

- Today
- April 3, 2019
- May 8, 2019
- 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!

Introduction to CCPA

How Did We Get Here?

Real estate developer, Alastair MacTaggart, proposed a California ballot measure, the California Consumer Privacy Act of 2018 ("CCPA").

Ballot Measure Proposed

9/1/17

While the state legislature was considering several privacy bills, the ballot measure received 629,000 signatures of CA residents - more than twice what is needed to appear in the November 2018 election.

Fall 2017 – June 2018

AB 375

After compromise between the ballot measure backers and state legislators, the CCPA (introduced as AB 375) passed in the Senate and Assembly, and was signed into law by Gov. Jerry Brown – hours before deadline for withdrawing the ballot measure.

Because the bill was passed quickly there are several areas that require clarification and correction. A "clean up" bill, SB 1121, corrected some of these issues. SB 1121 passed on the final day of the legislative session.

SB 1121

September 2018

Further amendments to the CCPA may occur during the 2019-2020 legislative session, and the AG is required to issue implementing regulations.

1/1/2020

Effective Date

SB 1121 postpones the AG's enforcement authority to June 1, 2020 (or, if earlier, six months after it issues its implementing regulations). Other provisions of the CCPA still go into effect on January 1, 2020.

The Scope of the CCPA

- The CCPA applies to **personal information** about California **consumers** or households.
  - **Consumer** is any natural person who is a California resident (includes customers, prospective customers, employees, business contacts, etc.).
- 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."

“Sale” Exclusions

- A “sale” of personal information does not include:
  - **Disclosures to a service pr**ovider that processes the information for a business purpose pursuant to a written contract that prohibits the service provider from using or disclosing the information for any purpose other than performing the services.
  - A **disclosure pursuant to a direction from the consumer** to disclose the personal information.
  - **Disclosures as part of a merger, acquisition, bankruptcy, or other transaction** involving all or part of the business, provided the information is used consistently with the notice provided.

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 – Mechanism for Information Requests

- **Request Mechanisms:** A business must provide at least two mechanisms for consumers to make information and access requests, including:
  - Toll-free phone number
  - Web site address
- **Timing:** A business must provide the requested information within 45 days of receiving a verifiable consumer request. This period can be extended another 45 days upon notice to the consumer.
  - *Note:* Another section of the law states that this time period can be extended "by up to 90 additional days where necessary, taking into account the complexity and number of the requests."

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.
  - ***Note:*** The private right of action for data breaches specifically does apply when information is covered by the GLBA, Cal. Financial Privacy Act, and DPPA.

Exemptions

- The CCPA does not apply to:
  - **Medical information** governed by the California Confidentiality of Information Act,
  - **Protected health information** that is collected by a covered entity or business associate governed by HIPAA's implementing regulations, and
  - A "provider of health care" under the CMIA or "a covered entity" under HIPAA to the extent that patient information is maintained in the same manner as medical information or protected health information.
- The CCPA does not apply to information collected:
  - as part of a **clinical trial:**
    - **subject to the Federal Policy for the Protection of Human Subjects**, also known as the Common Rule,
    - **pursuant to good clinical practice guidelines** issued by the International Council for Harmonisation, or
    - **pursuant to human subject protection requirements** of the United States Food and Drug Administration.

Enforcement

- Private Right of Action for Data Breaches: Any consumer whose nonencrypted or nonredacted personal information, as defined in California's data breach law, is subject to unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement reasonable security procedures and practices appropriate to the nature of the information may bring a civil action for the following:
  - $100-$750 per consumer per incident,
  - Actual damages, if greater than the $100-$750 amount,
  - Injunctive or declaratory relief, and
  - Any other relief the court deems proper

Enforcement

- **Notice Requirement for Private Suits:** Before bringing an action, however, 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 may not seek statutory damages.
  - If the business violates the terms of its express written statement, then the consumer may pursue an action to "enforce" the written statement and may claim statutory damages for each violation.
  - A consumer is not required to provide notice if seeking **actual damages**.

Enforcement

- **Enforcement by the Attorney General:** A business will be in violation of this title if it fails to cure any alleged violation within 30 days of being notified of its non-compliance. The Attorney General may bring a civil action against any business, service provider, or other person who violates the title.
  - Each violation may result in a $2,500 penalty
  - Each intentional violation may result in a $7,500 penalty
  - The Attorney General may also seek an injunction

What to Expect in 2019

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 has been conducting public forums for interested persons to provide testimony. Last forum is on March 5.
- In addition, AG accepting comments through March 8.
- Formal rulemaking process will also allow opportunity for public comment.

Efforts to Further Amend

- Hearing before California Assembly Privacy and Consumer Protection Committee held on February 20.
- California Chamber of Commerce, California Retailers Association, American Civil Liberties Union and others provided testimony.

Some Concerns Cited by Business Community

1. CCPA forces businesses to turn pseudonymous data into identifiable information.
2. CCPA creates the opportunity for any person in a household to potentially access unauthorized personal information about fellow members of that household.
3. CCPA fails to give consumers' options for nuanced and tailored deletion and opt-out choices.

Expansion of Private Right of Action?

- AG's position is that private rights of action are a "critical adjunct" to the AG's ability to enforce.
- Cal AG's office announced on Monday that they have worked with state Sen. Hannah-Beth Jackson to introduce a bill (SB 561) to expand the private right of action to any violations of the CCPA.
  - Bill would also eliminate 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.)

Questions

DrinkerBiddle®

Peter A. Blenkinsop

Partner | Washington, D.C.

peter.blenkinsop@dbr.com
Phone: (202) 230-5142

About

Peter Blenkinsop is a partner in the Government and Regulatory Affairs team at Drinker Biddle. He has more than 15 years of experience advising companies on compliance with privacy and data protection laws, and he co-chairs the firm's Information Privacy, Security and Governance (IPSG) group. Peter represents clients in the life sciences, health, nutrition, insurance, education, automotive and technology sectors, among others.

Peter works with clients in the development of privacy policies and procedures, including overarching privacy policies, and policies and procedures for sales and marketing, research and human resources. He also assists in the development of IT security policies and security incident response plans and procedures. Peter has worked with a leading nutrition company, a large university with campuses around the world, a large auto manufacturer, and dozens of the top pharmaceutical and medical device companies on privacy and security projects, analyzing specific programs and activities, providing advice on compliance with relevant laws, conducting large-scale privacy gap assessments to compare practices to legal requirements and best practices, and assisting organizations in development of data protection programs. He regularly advises on cross-border data transfer questions and matters necessitating the collection of personal data from outside the United States (such as international legal discovery).

Peter received his J.D. degree, magna cum laude, from Georgetown University Law Center, where he was an Associate Editor of the Georgetown Law Journal. He received his B.A. degree, cum laude, from Yale University, where he double majored in Economics and East Asian Studies.

Areas of Focus

Services

- Consortia Management
- Government and Regulatory Affairs
- Information Privacy, Security and Governance
- Clinical Research

Industries

- Health Care
- Pharma and Life Sciences
- Retail
- Technology
- Education

Credentials

Bar Admissions

- District of Columbia
- Maryland

Education

- Georgetown University Law Center, J.D., 2006, *magna cum laude*
- Yale University, B.A., 1999, *cum laude*

Organizations

- District of Columbia Bar Association
- International Association of Privacy Professionals

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

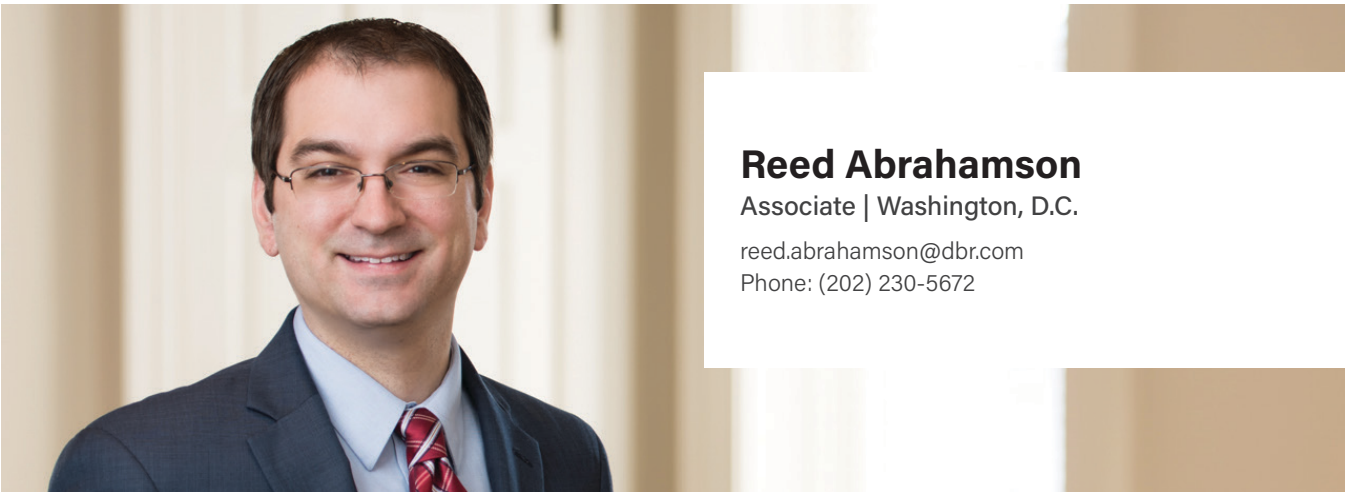
Court Admissions

- 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*

DrinkerBiddle®



Reed Abrahamson

Associate | Washington, D.C.

reed.abrahamson@dbr.com
Phone: (202) 230-5672

About

Reed Abrahamson assists clients with identifying and addressing data privacy and security risks in business operations. He has helped companies design and implement privacy and data security policies and programs, and advises clients on compliance issues related to HIPAA, CAN-SPAM Act, TCPA, and other privacy laws. Reed also has experience working with companies to respond to data breach incidents.

A United States Certified Information Privacy Professional (CIPP-US), Reed works with in-house teams to create frameworks for international transfers of regulated personal information, particularly from the European Union to the United States.

Reed also counsels clients on managing risk through appropriate policies and contractual arrangements, including drafting and modifying customer and consumer-facing privacy policies and statements. He has helped clients retain service providers and enter into arrangements with customers.

In addition, as a member of the firm's Consortia Management Team, Reed works on the formation, management, and representation of consortia in the life sciences industry that address matters of science, policy, law, and business operations. He assists in the creation of appropriate collaboration mechanisms and provides legal support for the day-to-day activities of these organizations.

Reed served as a law clerk to the senior judges for the District of Columbia Court of Appeals.

Areas of Focus

Services

- Consortia Management
- Government and Regulatory Affairs
- Information Privacy, Security and Governance
- Technology Transactions and Licensing

Industries

- Pharma and Life Sciences

Credentials

Bar Admissions

- District of Columbia
- Maryland

Education

- Georgetown University Law Center, J.D., 2012, *magna cum laude, Georgetown Immigration Law Journal*
- Yale University, B.A., 2008