Data Privacy and Cybersecurity

Data privacy and cybersecurity have never been more important to today’s businesses. As legal regimes governing data expand and risks to data intensify, our Data Privacy and Cybersecurity Practice provides holistic, proactive, and practical advice to clients.

Whether it is by assessing cybersecurity and data privacy risk, building privacy programs, helping clients navigate evolving regulatory frameworks, or aggressively litigating on behalf of our clients, we help organizations develop and defend secure and practical legal frameworks for the data they collect, use, analyze, and share. We offer a steady hand to companies preparing for, investigating, and responding to cybersecurity threats. In the event of an incident, we are sought-after crisis managers throughout the lifecycle of a response.

Hardening Your Compliance Infrastructure

As compliance rules continue to evolve, we provide practical, actionable advice on the patchwork of US and global requirements governing data privacy, particularly the California Consumer Privacy Act (CCPA), Illinois Biometric Privacy Information Act (BIPA), EU General Data Protection Regulation (GDPR), and other leading regulatory standards. We conduct ongoing preparedness reviews to evaluate safeguards and work to ensure that specific regulatory requirements are met in highly sensitive areas such as international data transfers and government contracting.

In the legislative arena, we create comprehensive strategies to give our clients a voice in future legislative debates and rulemakings governing privacy and data protection.

A Track Record in Privacy Litigation

Our team includes seasoned trial and appellate advocates with wide-ranging experience in complex commercial litigation, investigations, and compliance. We have successfully defended clients in numerous consumer class action claims under the CCPA and BIPA. Combining our BIPA experience with our California consumer class action work and CCPA knowledge gives our clients a critical advantage in adjusting to new requirements in privacy and data protection.

Experience That Adds Value

In addition to trial experts, our team includes former federal government lawyers, in-house counsel, and cybercrime prosecutors who understand what regulators are looking for in compliance investigations, how companies implement privacy and security requirements, and how oversight agencies will likely apply data privacy and cybersecurity legislation and regulations. As a result, we
quickly identify issues and risks that may impact clients’ business operations and help them adapt to change.

Responses Tailored to Client Needs

Recognizing that every organization has unique concerns about data privacy issues, we customize each approach to meet both legal and business goals. We are known for going above and beyond to understand our clients' businesses, and for collaborating seamlessly with internal teams including IT, legal, and compliance.

Working at the intersection of data privacy and cybersecurity, investigations, congressional matters, and class action litigation, we help clients make sense of the shifting data privacy and cybersecurity landscape to prepare for what lies ahead.

Experience

- Counsel and represent an international company in all aspects of its response to a cyber incident that was reported to have involved over 500 million customer records. This incident has been of considerable legal, business, and regulatory importance to the organization, and the company brought in Jenner & Block to serve as lead coordinating counsel in managing the response.

- Represent a facial recognition and data company in numerous class actions challenging its technology. The plaintiffs’ lawsuits raise a variety of claims, including alleged violations of the Illinois Biometric Information Privacy Act. We also advise the client with respect to inquiries from international data protection authorities in Europe and elsewhere.

- Counsel and represent a hospitality company with respect to a data-related property system incident. The company brought in Jenner & Block to serve as lead coordinating counsel in managing the incident and regulatory response. We also handled the resulting civil litigation and obtained a pretrial dismissal of the plaintiffs’ suits.

- Counseled and represented a financial institution in response to a ransomware attack, including managing the forensic response team in investigating the incident and remediating and hardening systems, negotiating response to regulators, coordinating communications strategy, and meeting disclosure obligations.

- Represented a major university in a putative class action in which the plaintiff alleged that, through its use of “remote test proctoring” software for student exams, the university allegedly collected scans of facial geometry in violation of BIPA. We won a motion to dismiss with prejudice based upon our development and aggressive pursuit of the argument that the university is a “financial institution” exempt from BIPA under Section 25(c) of the statute.
• Counseled and represented a manufacturing company in response to a cyber attack, including managing the forensic response team in investigating the incident and remediating and hardening systems, negotiating response to regulators, coordinating communications strategy, and meeting disclosure obligations.

• Counseled a law firm to perform a post-incident security assessment in order to remediate and harden systems in the wake of compromise attempts by a persistent threat actor.

• Providing an aerospace and defense company with cybersecurity preparedness and compliance advice.

• Counsel and represent a financial institution in response to a cyber attack on a software vendor involving a compromise of the client’s data, including coordinating with the forensic response team investigating the incident, negotiating response to regulators, coordinating communications strategy, and meeting disclosure obligations.

• Represent an artificial intelligence company in putative class actions involving the collection, storage, and use of voiceprints in violation of BIPA.

• Represented hospitality company in two separate putative class action suits arising from property system incident and won dismissal with prejudice in both cases.

• Representing major private university in multi-district litigation arising from data incident involving a university vendor.

• Representing health care industry client in putative class action arising from data incident involving a third-party vendor.
Co-Chairs

David Bitkower
Co-Chair
dbitkower@jenner.com
+1 202 639 6048

Madeleine Findley
Co-Chair
mfindley@jenner.com
+1 202 639 6095

Shoba Pillay
Co-Chair
spillay@jenner.com
+1 312 923 2605

Related Capabilities

Aerospace and Defense
Business Litigation
COVID-19
Cannabis
Class Action
Communications, Internet, and Technology
Congressional Investigations
Consumer Brands
Content, Media, and Entertainment
Culture Risk and Sensitive Investigations

ESG: Environmental, Social, and Governance

Education

Election Law and Redistricting

Energy

Fintech and Digital Assets

Food and Beverage

Government Contracts

Government Controversies and Public Policy Litigation

Insurance Recovery and Counseling

Investigations, Compliance, and Defense

Investment, Private Equity, and Hedge Funds

Law Firms and Professional Services

Life Sciences

Markets and Trading

National Security, Sanctions, and Export Controls

Post- *Dobbs* Task Force

Real Estate and Hospitality

State Enforcement and Regulation