SheppardMullin

Privacy and Cybersecurity

Nearly every facet of a company's operations is subject to a complex array of privacy and cybersecurity challenges. Our clients rely on our in-depth understanding of the law and our ability to partner with them to find practical ways to mitigate risk.

Our 30+ global, interdisciplinary Privacy & Cybersecurity Team includes some of the most respected lawyers in the privacy space, including a lawyer who literally "wrote the book" on data breach, award-winning privacy class action litigation practitioners, and leading incident response practitioners. Not only are many of our team members CIPP certified by the IAPP, but we are active members in the organization, from committee participation to running privacy trainings, underscoring our commitment to the privacy field.

Sheppard Mullin's Privacy Team accolades include being named Law360's Cybersecurity & Privacy Practice Group of the Year; highly ranked by Legal 500 USA (Cyber Law), Legal 500 Europe (EU Data Protection); and one of only 25 firms ranked in the inaugural ATL Top Law Firm Privacy Practice Index.

Our lawyers have experience in the full breadth of privacy and cybersecurity matters. From high-profile data breaches, regulatory investigations, complex litigation, compliance counseling, we assist a broad array of clients across a spectrum of industries. Clients rely on the integrated nature of our global offering and our ability to address privacy and security issues faced by global brand and retail clients at a senior level.

Areas of Experience:

Litigation

Our privacy litigators defend clients from landmark class and individual actions based on cutting edge legal theories to claims brought under long-standing privacy laws. Clients rely on the Sheppard Mullin team in what often become bet-the-company cases. From large cases to small, our team is focused on getting the best result for our clients.

Our work includes defending clients in consumer class actions, competitor lawsuits, and government enforcement actions related to privacy claims. We regularly handle complex, high-profile privacy lawsuits and landmark cases involving constitutional privacy rights, state law claims like California's Song-Beverly and Shine the Light Acts, Illinois Biometric Information Privacy Act (BIPA), claims asserted under the Computer Fraud and Abuse Act (CFAA), and California Invasion of Privacy Act (CIPA). We also represent clients in cases involving penal code wiretapping and call recording claims, the federal Telephone Consumer Protection Act, RICO claims related to privacy, and various other state and federal statutes.

Representative cases include protecting and defending clients in claims that allege violations in handling fingerprints and face prints, those that argue that websites have "eavesdropped" on chatbot conversations, and defending clients in complex and high-profile multi-jurisdictional cases that follow in the aftermath of data breaches.

In all of these matters, our practitioners provide practical and knowledgeable support. What sets us apart is our dual expertise. Our litigators are also privacy counselors, advising clients on compliance with the very privacy laws and issues that form the crux of the complaint. This lets us to craft a more strategic defense, tackling tough questions that lie at the heart of litigation. Another differentiator on which our clients rely is our realistic and practical approach to cases, especially those filed by opportunistic plaintiffs' counsel. We challenge plaintiffs' counsel to stand by their case theory, knowing that the prospect of time-consuming and costly litigation often deters them from pursuing the case further when they realize there's no easy money to be made.

Regulatory Enforcement

The Sheppard Mullin team assists clients in a wide variety of investigation matters, relying on their experience to successfully represent clients before a wide variety of regulatory bodies.

Our practitioners have experience in assisting clients in investigations brought by an alphabet soup of state and federal regulators. From investigations before the Federal Trade Commission, Federal Communications Commission, Securities and Exchange Commission, Department of Health and Human Services - Office for Civil Rights, and variety of financial services regulators (Consumer Protection Bureau (CFPB), Federal Reserve Board (FRB), New York Department of Financial Services (NYDFS) and others), we are zealous advocates for our clients. We also regularly assist clients in representations before committees of the US Congress.

Additionally, whether in the wake of data breach notifications or other public matters, our clients rely on our ability to advocate on their behalf in investigations brought by state Attorneys General and other regulators.

Sheppard Mullin also has an active government regulatory practice. Our team helps our client navigate growing requests by government to private data. We help clients balance competing priorities and navigate sensitive negotiations around such disclosures with law enforcement, national security, and other government agencies. We use our connections with law enforcement, the intelligence community, and the national security establishment to provide a discreet, strategic, and comprehensive responses.

Incident Planning and Response

We leverage our experience in data breach response to help clients prepare for what is often not an "if" but a "when" for incident response. Our knowledge of our clients and their practices helps us guide them through incidents effectively using tools to help mitigate and minimize risk.

To assist clients in preparing for potential incidents, our team conducts comprehensive reviews of clients' data storage and security practices, policies, procedures, third-party agreements, and regulatory requirements to plan for data security incidents. We use our connections with forensic security consultants, crisis communications firms, identity-theft protection providers, and law enforcement agencies to benefit our clients. Through table-top exercises, we evaluate clients' preparedness for cyberattacks or other data incidents.

In the wake of an incident, our team provides strategic, comprehensive support. This includes advising on forensic investigations, and crisis communications. We also interact with law enforcement and regulators on our client's behalf, and assist in compliance with multi-jurisdictional, global breach notification obligations. Our team is always mindful during the response that litigation or regulatory inquiries are possible, and carefully strategize responses with this in mind. Should claims or investigations begin, we are well poised to assist our clients.

We have supported clients through a wide variety of incidents, including some of the most sophisticated and largest ransomware attacks. Our work includes advising on negotiations with threat actors, proof of life, and decryption. We collaborate with leading third-party intermediaries to ensure secure communication and negotiation with threat actors. If necessary, we assist in establishing a bitcoin account for ransom payment, checking OFAC listings, liaising with the FBI in advance of the payment to ensure it is not flagged and prevented by law enforcement, and to tumble the payment once it is initiated.

Compliance

Our team of privacy professionals has a breadth of experience helping companies of all sizes and across various industries stay up to date and develop and implement a tailored compliance strategy.

Our lawyers are leaders in the field, and assist major brands, ad agencies, and research companies in interacting with consumers while complying with the ever changing, complex patchwork of privacy laws. When assisting companies with compliance projects our work is informed by our depth of knowledge in US and global privacy laws, including the California Consumer Privacy Act and similar state laws, CalOPPA, the Song Beverly Act, state telemarketing laws, TCPA, CAN-SPAM, COPPA, HIPAA, GLBA, GDPR, and more.

We provide a full suite of assessment and remediation services and assist companies in implementing “privacy by design” principles into their organizations, technologies, products, and services. We understand that designing technologies, products, data transfer mechanisms, apps, and websites with privacy and security protections embedded will help to mitigate future legal and regulatory risks. Work we do includes assisting clients with privacy policies and procedures, training, and developing practical and implementable remediation solutions.

Our team has experience in a variety of industries. From health care, financial services, retail, and representation of companies who contract with government entities, we work with a wide breadth of clients. For those selling to the government, we leverage our strong ties with government officials to guide clients through the complex laws, standards, and regulations related to cybersecurity and cloud computing.