SheppardMullin

Privacy and Cybersecurity

Nearly every facet of a company's operations—from internal employment practices to online operations, data collection and customer contact—is subject to a complex array of legal and business challenges related to privacy. Companies need practical advice from experienced counsel who thoroughly understand privacy law to prevent potential disasters. Sheppard Mullin is uniquely qualified to help.

Our 30+ global, interdisciplinary Privacy & Cybersecurity Team includes some of the most respected lawyers in the privacy space, including a former U.S. Department of Homeland Security deputy general counsel, a lawyer who literally "wrote the book" on data breach, award-winning privacy class action litigation practitioners, and leading EU-based data protection experts. Many of our team members are CIPP-US and CIPP-EU certified by the IAPP, 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, and 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.

We partner with clients to help them extract value from the data they collect, while identifying and addressing regulatory compliance requirements, and ensuring that data is appropriately protected. Our lawyers have experience responding to high-profile data breaches, including state-sponsored attacks, and the regulatory investigations, Congressional oversight and litigation that often follow such incidents. We litigate major privacy and security related class actions. We provide strategic counsel to help companies understand emerging developments in this rapidly changing area of law, particularly with EU data collection and international data transfers. As data becomes more entwined with the enterprise value of businesses, we conduct data and privacy compliance due diligence in connection with mergers and acquisitions and other corporate and strategic transactions.

We pride ourselves on the integrated nature of our global offering. We address the privacy and security issues faced by our global brand and retail clients at a senior level, and provide central coordination to craft an integrated global strategy which recognizes and respects regional differences. These differences often reflect vastly different consumer perceptions of privacy, which may go far beyond regulatory distinctions.

Our Expertise

Our global, interdisciplinary team of lawyers can help you anticipate privacy and security issues, and respond to privacy investigations, litigation, cybercrimes and network intrusions, including:

Biometric Information Privacy Act (BIPA)

The Biometric Information Privacy Act (BIPA) is an Illinois statute that took effect in October of 2008 and protects against the unlawful collection, use, and storage of biometric information, such as fingerprints, iris scans, and face prints. BIPA is one of three state laws that regulate collection of biometric information, but is the most stringent in terms of the consent, notice, and disclosure protocols private entities must follow. BIPA's reach has extended well outside of Illinois, and Sheppard Mullin represents companies across the country who

collect or otherwise use the biometric data of individuals located in Illinois. Our work includes both defense in BIPA litigation, as well as counseling for setting up biometric information collection and use programs. Unfortunately, even when best practices are followed, BIPA litigation is still a real possibility and you need a skilled advocate in your corner.

At Sheppard Mullin, attorneys on our Privacy and Cybersecurity Team have litigated over a dozen BIPA cases for clients in an array of industries. Our attorneys have not only spent a significant time litigating such cases, they also utilize their unique expertise counseling clients on how to mitigate risk and avoid them. When companies are confronted with alleged violations of BIPA, they turn to Sheppard Mullin for assistance as a leader in the field with a proven track record of obtaining great results for our clients through a strategic combination of considered approaches.

Blockchain Technology and Digital Assets

Since the financial crisis, innovation in the financial services industry has surged. Meeting at the intersection of Wall Street and Market Street are new financial technologies including blockchain and digital currencies such as Bitcoin, Ether and Litecoin. Across the banking, money services, securities, and video game industries, data-driven startups and established financial companies are easing payment processes, reducing fraud, saving users money, promoting financial planning and ultimately moving a giant industry forward. We understand blockchain technology, and the vital roles that privacy and cybersecurity play in the blockchain industry. We also help companies using blockchain technology address currency and lending issues, intellectual property, taxation, securities and the transactional needs as they develop these new technologies.

Computer Fraud and Abuse Act Litigation

We represent companies who have been targeted by hackers, former employees or competitors looking to profit from gaining access to trade secrets or other proprietary or sensitive data. We have experience in asserting claims under the Computer Fraud and Abuse Act (“CFAA”) to combat unauthorized access to corporate computer networks, servers and email accounts, and in asserting additional claims for misappropriation of trade secrets and violations of the Stored Communications Act.

Consumer and Communications Privacy

We have been a leader in the advertising and consumer protection field for decades. Our lawyers help major consumer brands, advertising agencies, and market research companies interact directly with consumers while respecting a myriad of complex laws, including the California Consumer Privacy Act, which came into effect on January 1, 2020. These include the ever-changing realm of marketing through email and text communications. We assist clients to develop compliant marketing and information collection programs, develop internal policies for safeguarding personally identifiable information, create privacy compliance policies, procedures, monitoring programs, and reporting plans, represent clients in litigation involving use of consumer information, and counsel clients with respect TCPA, CAN-SPAM, COPPA, and other communications regulations.

Cybersecurity for Government Contractors

Our team combines experts in both cybersecurity and government contracts law to provide unparalleled advice to companies selling products and services to the government, as they face rapidly-changing cybersecurity standards and requirements from a variety of government agencies. With deep relationships to government officials, we are called on by some of the largest and most prominent government contractors to guide them through the maze of laws, standards, and agency regulations regarding cybersecurity and cloud computing and assist them with government-specific aspects of incident response.

Data Breach and Incident Response, Investigation, Communication and Litigation

We provide a strategic, comprehensive response to complex and high-profile data security incidents, including advising clients regarding forensic security investigations, crisis communications and public relations strategies, interactions with law enforcement and state and federal regulators, industry groups and payment card industry players, complying with federal and state breach notification obligations, and defending them in the federal and state regulatory investigations and class-action litigation that may follow. We also advise clients on investigating and responding to breaches affecting their vendors and business partners, and on "ransomware," "DDoS" and other cyber incidents which do not involve the disclosure of consumer data but which adversely impact business operations. In addition, we advise clients on indemnification and other rights and remedies under vendor or other third-party agreements, and on cyber-insurance coverage matters.

Data Security Incident Response Planning

We help clients plan for data security incidents by conducting a thorough review of their data storage and security practices, their existing policies and procedures, third-party agreements, and regulatory requirements. We help clients leverage our relationships with forensic security consultants, crisis communications firms, identity-theft protection providers and law enforcement agencies. We conduct table-top exercises to help clients assess their readiness to respond to cyberattack or other data incident.

Federal and State Regulatory Investigations of Privacy and Data Security Practices

Government regulation of privacy and data security matters is rapidly expanding, as an ever-growing list of agencies acquires new regulatory powers and intensifies investigative focus. We help clients respond to investigations, inquiries and enforcement actions from the Federal Trade Commission, Federal Communications Commission, Securities and Exchange Commission, Department of Health and Human Services - Office for Civil Rights, National Highway Transportation Safety Board, committees of the U.S. Congress, State Attorneys General and other regulators. We advise clients on how to respond to sensitive requests for information sharing from law enforcement agencies. We represent clients in Congressional testimony and investigations, and help government contractors comply with a growing list of cybersecurity and insider threat rules. We help clients navigate this complex regulatory environment -- from compliance with existing requirements to the submission of comments on proposed new rules, to representing clients in investigations before Congress and government agencies. We understand industry- specific regulations, including those that govern financial data (Gramm–Leach–Bliley Act), health data (HIPAA, GINA), and the Children's Online Privacy Protection Act (COPPA), new federal laws such as the Cybersecurity Act of 2015 and the Cybersecurity Information Sharing Act, as well as

specialized state privacy laws.

Global Data Protection, GDPR and International Information Transfers

We counsel clients on cross-border data transfers, including compliance with EU, Canada, and other international data privacy laws. We help clients achieve certification under the US-EU Privacy Shield, and routinely handle EU standard contractual clauses and US-Swiss Privacy certifications for clients. With offices in London, Brussels, Shanghai, Beijing, and Seoul, we have local expertise in privacy and data security matters in the UK, EU and its member states, China, and Korea, and are closely monitoring any developments in data protection and privacy law that may arise as a result of Brexit.

Our European experts advise clients on the steps required to ensure compliance with the European General Data Protection Regulation, which came into effect on 25 May 2018. We help build new processes and compliance policies, we advise on IT requirements and architecture to ensure that companies are able to discharge of their newly imposed obligations under the GDPR, as well as to deal effectively with rights of individuals. We also advise companies on how to efficiently change existing policies in the most cost-effective way to bring them in line with the GDPR globally. The wide jurisdictional scope and the anticipated increased risk of fines, investigations and litigation made this a high-priority area for companies that handle consumer and human resource data of individuals in the European Union.

National Security, Government Data Requests and Law Enforcement Demands

Law enforcement and national security agencies increasingly look to private companies to share information and to assist in government investigations by enabling government access to private data. Our lawyers, including a former deputy general counsel for the Department of Homeland Security, have experience in helping clients balance competing priorities and in navigating these sensitive negotiations with law enforcement, national security and other government agencies. We leverage our contacts with law enforcement, the intelligence community and the national security establishment to provide a discreet, strategic, comprehensive response to sensitive state-sponsored and/or criminal data security incidents.

Online Defamation and Freedom of Speech Litigation

Our First Amendment lawyers represent online, media and other companies in defamation cases. Our team includes former top in-house counsel at a major internet company with extensive experience in online speech, defamation, privacy and ISP immunity matters, as well as experienced First Amendment litigators.

“Privacy by Design” in New Technologies or Product Offerings

We help companies implement “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.

Privacy Litigation

We vigorously represent clients in consumer class actions, competitor lawsuits, and government enforcement actions involving privacy claims. We have a distinguished track record in handling complex, high-profile privacy lawsuits. Our lawyers have handled landmark cases involving constitutional privacy rights, state law claims such as California's Song-Beverly and Shine the Light Acts, penal code wiretapping and call recording claims, the federal Telephone Consumer Protection Act, RICO claims relating to privacy and various other state and federal statutes, as well as related vendor indemnification actions. Our recent victories include halting the expansion of certain privacy claims to new technologies and new jurisdictions and obtaining the dismissal of a multi-billion dollar digital privacy class action involving user profiles for a major internet company.

Privacy Policies and Website Terms and Conditions

We advise clients on internal privacy policies and procedures relating to both consumer and human resources data. We draft public-facing privacy policies to implement and reflect our clients' objectives and practices, and help them train their employees on compliance with these policies. We understand that a public-facing privacy policy is both a legal and marketing document and a carefully crafted approach to complying with legal and regulatory requirements, all while reflecting each client's unique brand and voice.

Privacy and Security in the "Internet of Things"

With the rise of the Internet of Things (IoT), virtually all of the things we use in daily life will collect enormous amounts of data that can be communicated to other devices and other parties. We advise clients across a wide range of industries – from automobile manufacturers developing connected car technologies, to fashion and retail industry clients developing wearable technologies, eHealth and telemedicine companies communicating biometric data – on the privacy and security issues presented in this interconnected environment. Our team understands the wide range of industry sectors that make up the IoT, and includes lawyers with expertise in the areas of data protection, telecom, intellectual property, media, life sciences and healthcare.