Cybersecurity, Privacy and Sensitive Technologies

Skadden

For more than 20 years, Skadden has helped clients navigate the rapidly changing cybersecurity, privacy and technology landscapes to minimize their legal risk, as well as maximize their revenue opportunities.

We also help clients address the complex issues at the intersection of technology, privacy, national security, intelligence and law enforcement. Based on extensive experience working with U.S. and foreign government agencies and regulators, we identify the legal risks associated with cyber- and other technology-related security concerns and assemble and coordinate multidisciplinary teams of advisers across the firm to address the universe of legal, regulatory and legislative issues faced by clients.

The breadth of our skills in cybersecurity and privacy law and the extent of our technology experience and business insights has earned the confidence of our clients to call on us both before and during a cyberattack. Skadden has been named among the top firms for cybersecurity and data privacy issues in "BTI Law Firms Best at Cybersecurity: Corporate Counsel Rank the Law Firms Leading the Charge on Change.

Cybersecurity

Skadden offers substantial experience guiding companies through all facets of cybersecurity, including developing policies and procedures before an incident arises, addressing the important actions immediately following breach situations, and navigating the federal and state government investigations and private litigation that increasingly accompany cybersecurity incidents or other breaches involving personal information. We counsel clients on board and leadership preparedness, cybersecurity preparedness reviews, incident response, federal government engagement and regulatory compliance.

Preparedness

Skadden's Cybersecurity, Privacy and Sensitive Technologies Group works with clients to identify and assess cyber risks from a legal perspective, drawing on our wide range of experience conducting such assessments. We counsel executive and board leadership on cybersecurity preparedness and assist clients in creating and reviewing incident response plans, conducting cybersecurity audits, developing cybersecurity governance practices, providing employee training and assessing insurance needs.

Development and Review of Security Incident Response Plans (SIRP)

Studies have shown that companies that have a tested SIRP in place respond more efficiently and effectively to an attack — a key factor in risk mitigation. We help clients create SIRPs or review and "table test" existing ones to ensure they reflect best practices and address the practical and legal issues most likely to arise around an incident. Because the quality of a SIRP and how it was executed will be a likely focal point of regulatory actions and litigation, building this plan from a legal perspective is essential.

Rapid Response

When a company discovers it is the victim of a cyberattack, every moment is critical. Companies not only must contain the attack and mitigate the damage, but also quickly manage demands from the media, government officials, customers, business partners and shareholders. Companies must be prepared for the reality that the media might break the news of an attack before a company is able to gather all the relevant facts, and that regulators and government officials are demanding faster response times and immediate alerts. The rapidity and efficiency with which a company responds to a cyberattack is now a subject matter of regulatory inquiry and claims

asserted by private plaintiffs. Skadden's multidisciplinary Cyberattack Rapid Response Team (CRRT) has the knowledge to help companies manage an attack and minimize legal exposure and the experience to help them uncover and address legal vulnerabilities in an efficient and cost-effective manner. Our team handles incident response, federal government engagement and regulatory compliance and advises on data breach notification requirements.

Cybersecurity and M&A

Due diligence has long been a critical tool for uncovering and protecting against key risks in a transaction. Cybersecurity due diligence requires a custom approach. As with any diligence effort, the scope will depend on the transaction timeline as well as the target company's industry, the value of its digital assets, its regulatory environment and its cyber-risk profile. Our team has developed a set of due diligence questions, and an overall approach to cybersecurity due diligence that helps clients assess these risks.

Enforcement and Litigation

Skadden offers a sophisticated practice, led by former federal prosecutors and experienced trial and appellate lawyers, focused on cybersecurity and privacy litigation. We represent clients in class actions, complex civil litigation and government and internal investigations. The key issues in enforcement actions and litigation following a cyberattack are how the company managed its cybersecurity planning before the incident and how it responded during the attack. Companies should expect questions about their cybersecurity governance structure, the level of engagement by C-suite executives and board members, and the quality of the company's crisis response plan. Companies should likewise be prepared for government and private plaintiffs to scour the company's internal and public statements about cybersecurity risk in search of potentially damaging statements.

In today's legal and regulatory environment, litigation can threaten a company's very existence. Skadden has extensive experience with such complex, "bet-the-company" matters, and we are widely recognized for our ability to handle our clients' most critical litigation issues. We have been widely recognized for our successes on behalf of clients, including being named *The American Lawyer*'s 2018 Litigation Department of the Year in the Regulatory/White Collar category and, for the ninth consecutive time, Skadden was named to BTI Consulting Group's 2019 list of top litigation law firms — The BTI Fearsome Foursome — and named as a Powerhouse for Securities and Finance Litigation in the BTI Litigation Outlook 2020.

Cybersecurity Audits

In any regulatory enforcement action or litigation, the regulator or private plaintiff will rely on the documented record to establish the company's negligence in managing cybersecurity or usage of personal information. We review clients' documentation relating to cybersecurity and privacy to help determine whether (i) the company has made statements that are inconsistent with, or overstate, its cybersecurity planning; (ii) external consultants highlighted proposals or concerns that were not adequately addressed; and (iii) employees are properly notified of their obligations when handling data and sensitive information. We conduct this review through a litigation lens to mitigate those potential concerns as part of a company's preparedness program. As part of this exercise, we also review whether a client's use of personal information, including internal and external data flows, is consistent with its stated policies and regulatory obligations.

Development and Review of Cybersecurity Governance Models

Regulators and private plaintiffs carefully scrutinize a company's cybersecurity governance to assess whether information security officers had clear accountability and access to senior management and the board, and whether the board was sufficiently informed. We help clients develop tailored cybersecurity governance practices and review the governance that clients already have in place, advising on whether changes may be warranted to align a client's governance with regulatory expectations and best practices.

Risk Assessment Analysis

We work with clients to identify and assess cyber-risks from a legal perspective. This includes determining a company's most valuable assets, how they are protected and who can access that information. Where clients already have conducted such an assessment, we review it to determine compliance with accepted practices.

Policies and Procedures

An increasing number of states and regulators now require formal written cybersecurity plans. Skadden has experience creating and reviewing all of the policies and procedures companies require, including external-facing security policies, internal policies guiding the use of personally identifiable information (PII) and cybersecurity, statements to be used in marketing collateral regarding security policies, written information security policies (WISPs) and language regarding cybersecurity to include in third-party contracts.

Cybersecurity, Privacy and Sensitive Technologies

Continued

Insurance

Our insurance team works with clients to review existing policies to determine whether cyber insurance is warranted, helps clients negotiate coverage and advises on the scope of coverage if an attack occurs.

Employee Training

While companies generally design and implement cybersecurity training internally, we work with clients to make sure the scope and level of training would satisfy a regulatory inquiry and best protect the company if its practices were challenged in a litigation.

Vendor Management Assessment

We review clients' vendor management processes to determine if appropriate steps are in place to asses cybersecurity risk are in place, and review the client's form agreements and third-party vendor agreements to determine if the client is adequately protected with respect to cybersecurity incidents. We also help clients assess their data breach notification obligations under their existing agreements.

Work With Forensics Experts

Skadden works with clients' forensic experts to evaluate cyberattacks and determine the best approach to remediation efforts. We have strong working relationships with the leading forensics providers and can help clients select the appropriate teams given their specific needs.

Law Enforcement and Regulators

The Skadden team includes former government officials who can advise clients on the roles of various agencies, including regulators and law enforcement, and appropriate ways to work with them. Skadden has extensive experience with numerous agencies, including the FBI Cyber Division, the Computer Crime and Intellectual Property Section of the Department of Justice, the Secret Service, the Department of the Treasury, the Department of Homeland Security and various independent regulatory agencies.

Data Breach Notification

Our attorneys stay up-to-date on all current state and federal data breach notification requirements. We can rapidly advise clients on navigating the myriad state data breach notification requirements, including determining whether notice is required to residents or local officials, drafting the appropriate breach notice letters, and assessing when they should be disseminated.

Managing Public Disclosures

Skadden has a long history of helping clients make appropriate public statements during a crisis. In the event of a cyberattack, companies must review all public statements to ensure that they are consistent with legal requirements and do not inadvertently increase risk. We have close working relationships with communications and public relations firms with experience in cyberattack response.

SEC and Regulatory Disclosures

Skadden's SEC Reporting and Compliance attorneys are knowledgeable on SEC and regulatory rules, and can quickly help clients assess whether disclosure is required under SEC filings or as a result of the company's regulatory obligations, and draft any necessary disclosures.

C-Suite and Board Support

Our attorneys routinely advise boards on critical company matters, and we have the experience to advise senior management and boards on cyberattacks, the company's risk exposure and the path forward.

Privacy and Data Protection

Privacy Advisory Services and Compliance

Companies are gathering and storing increasing amounts of information about their customers, and finding new ways to monetize that information, fueled in part by an increase in innovative mining and analytic tools. These monetization opportunities have drawn the close attention of regulators, government officials and plaintiffs' lawyers. Companies that do not have robust privacy programs, and do not comply with such programs, are facing increased legal exposure, including the possibility of long-term regulatory consent decrees. For over 20 years, Skadden has assisted clients in navigating the rapidly changing privacy and technology landscapes to minimize their legal risk and maximize their revenue opportunities.

California Consumer Privacy Act

The California Consumer Privacy Act (CCPA) has imposed a number of privacy requirements on companies that process data of California residents, including those that are not physically located in California. The Skadden privacy team works with clients to determine if the CCPA applies to their business, to develop compliance programs, to train employees on CCPA issues, and to address CCPA issues as they arise.

Global Privacy Policies

Many of our clients use and distribute data across multiple geographic regions and across multiple device types. We counsel clients on establishing and maintaining global privacy policies that are customized to the requirements of individual countries. As part of these engagements, we meet with clients to discuss their current and future use of personal data to establish an overall strategy and then use this information to develop a global privacy approach. Once these privacy structures are in place, we work with clients on an ongoing basis to update them as laws and regulations, or the company's own business needs, evolve.

Cybersecurity, Privacy and Sensitive Technologies

Continued

EU General Data Protection Regulation

The EU General Data Protection Regulation (GDPR) has imposed a variety of new requirements on companies processing the data of EU residents. Skadden works closely with clients to help them understand the scope and applicability of the GDPR to their business, and to design compliance programs that meet the GDPR requirements. This includes working with clients to manage the evolving requirements of cross-border data flows.

Privacy Audits and Compliance Programs

Regulators and plaintiffs' lawyers increasingly are focusing on how companies collect and use personal information. Their focus is not only on compliance with privacy laws, but also on whether a company is using personal information in a manner that is consistent with its privacy policies and marketing materials. When regulators such as the Federal Trade Commission (FTC) have brought enforcement actions, they are not merely pursuing "bad actors;" they also are bringing enforcement actions against companies that may have inadvertently acted in contrary way to what they represented to their consumers.

A privacy audit helps companies eliminate these potential areas of liability and engenders a culture of vigilance with respect to privacy compliance that extends beyond the audit itself. As part of our privacy audits we:

- Ensure the client collects and utilizes PII in a manner that complies with applicable legal requirements as well as statements it has made to customers and employees;
- Ensure the company is in compliance with any data use restrictions imposed by third parties, including social media platforms;
- Establish internal processes and create policies to ensure that PII always is used in a manner that complies with applicable legal requirements and external and internal disclosures;
- Establish a data map of how information is collected, used, managed, stored and distributed internally and externally that can be updated and monitored on a regular basis;
- Establish a process for ensuring local law compliance and, outside the U.S., for interacting with applicable data protection authorities;
- Establish ongoing training and monitoring programs; and
- Review and/or create all necessary policies and procedures.

Regulatory Compliance

We advise clients on the steps necessary to comply with all privacy regulations, including the Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, the Fair and Accurate Credit Transactions Act, the Children's Online Privacy Protection Act (COPPA), the CAN-SPAM Act, and the Telemarketing Sales Rule and the Telephone Consumer Protection Act. We counsel clients on how industry trends and new protocols may impact the use of personal information and help them find innovative solutions that allow them to utilize the information they have without violating any legal requirements. Our attorneys also track developments at the state and federal levels to ensure that our clients are fully informed about, and fully compliant with, any changes in the legal and regulatory environment.

Policies and Procedures

Skadden works with clients to create and review a wide range of privacy compliance documents, including:

- External facing privacy policies;
- Internal employee policies guiding the use of PII;
- Statements to be used in marketing collateral regarding privacy policies;
- Written Information Security Programs (WISPs);
- Cross-border data flow documentation; and
- Language regarding privacy to include in vendor agreements.

Data Monetization

Our clients are increasingly looking for ways to monetize the data they hold, including through new analytics tools. We negotiate third-party vendor agreements in this space and advise clients on whether their planned programs comply with their privacy policies and applicable laws.

Privacy by Design

Regulators expect companies to engage in "privacy by design" — the concept that privacy consideration should be an integral part of the development process for any product or service. We work with clients to develop privacy by design programs that minimize the legal risk that PII is used in a manner that might draw regulatory scrutiny or invite a lawsuit. Companies that engage in privacy by design programs find that they save money by avoiding the need to backfill privacy protections after a new product or service has been finalized.

Sensitive Technologies

Skadden offers substantial experience assisting companies with all facets of sensitive technologies, including managing global supply chains, addressing intelligence and law enforcement inquiries, engaging with government contracting officials, developing policies and procedures before issues arise, and counseling before and during congressional or regulatory inquiries. For clients that work with the U.S. government, we advise on compliance with regulations and standards related to safeguarding government information from cyberattacks, including the National Institute of Standards and Technology (NIST) Special Publications and Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012, and provide guidance for obtaining certification under the Defense Department's Cybersecurity Maturity Model Certification (CMMC) program. Our attorneys address novel questions that arise due to technological advances in encryption, the global nature of data storage, government surveillance capabilities and authorities, and mitigation of the associated legal risk. We work closely with nondefense-focused technology companies that increasingly find themselves a focus of intelligence, law enforcement and homeland security officials. We routinely help companies navigate contracting, regulatory and investigative issues in the U.S. and abroad. Our unique experience in senior government positions as well as in business roles in both start-up and established public technology companies provides a critical perspective on how to address the full range of increasingly nuanced issues that arise at the nexus of technology, information and security.