Cybersecurity and Privacy

Skadden

Cyberattack preparedness, coupled with a well-developed and tested Security Incident Response Plan (SIRP), is essential for minimizing the legal, operational and reputational risk arising from cyber threats. Engagement with outside counsel who know the legal and regulatory landscape and the key areas of potential liability exposure is a critical part of any company's cybersecurity strategy. The breadth of our skills and the extent of our experience has earned the confidence of our clients to call on us both before and during a cyberattack. In 2017, Skadden was 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."

Privacy Advisory Services and Compliance

Companies are gathering and storing increasing amounts of information about their customers, and finding innovative ways to monetize that information. This has been fueled, in part, by an increase in innovative mining and analytic tools that are available to companies. However, these monetization opportunities have drawn the close attention of regulators, government officials and plaintiffs' lawyers. Companies that do not have robust privacy programs are facing increased legal exposure, including the possibility of long-term regulatory consent decrees.

For over 20 years, Skadden has added value to clients by assisting them in navigating the rapidly changing privacy and technology landscapes to minimize their legal risk, and helping them maximize their revenue opportunities.

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. We take this information and 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.

Our group also works with clients to understand and comply with cross-border data flow requirements in a manner that is best suited for their business needs. With respect to data transfer out of the EU, we advise clients on model contracts and binding corporate rules, and assist clients with certifying to the EU-U.S. Privacy Shield.

EU General Data Protection Regulation

The upcoming EU General Data Protection Regulation (GDPR) will impose a variety of new requirements on companies accessing the data of EU residents. Skadden works closely with clients to help them understand the scope and applicability of the GDPR and to design compliance programs so that they are prepared to meet the GDPR requirements when they go into effect in 2018.

Privacy Audits and Compliance Programs

Regulators and plaintiffs' lawyers increasingly are focusing on how companies collect and use personal information. Their focus not only is on compliance with privacy laws, but also on whether the company is using personal information in a manner that is consistent with their 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." Rather, they also are bringing enforcement actions against companies that may have inadvertently acted contrary to what they represented to their consumer.

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 personally identifiable information (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 closely track developments at the state and federal levels to ensure that our clients always 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 "big data" 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 "back-fill" privacy protections after a new product or service has been finalized.

Cybersecurity and Privacy
Continued

Cybersecurity Preparedness Services

Companies today appreciate the importance of implementing the most up-to-date information security technology to prevent or minimize the impact of a cyberattack. But a company's cyber-preparedness cannot end there. The key issues in enforcement actions and litigation following a cyberattack are how the company managed its cybersecurity planning before the attack, and how it responded during an 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. In building their case, the government and private plaintiffs also will scour the company's internal and public statements about cybersecurity risk, looking for potentially damaging statements.

To best manage a cyber-incident, companies today need to build a "legal firewall." Skadden's Privacy and Cybersecurity Group has the experience to help companies uncover and address their legal vulnerabilities in an efficient and cost-effective manner.

Development and Review of Security Incident Response Plans (SIRP)

One of the most important steps a company can take before a cyberattack is to develop and test a 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 existing ones to ensure they reflect best practices and address the legal issues most likely to arise around an incident. Because the quality of the SIRP and how it was executed will be a likely focal point of regulatory actions and litigation, building the SIRP from a legal perspective is essential. We also routinely work with clients to "table test" their existing plans, pointing out legal and practical issues that may arise during an attack.

Cybersecurity "Audits"

In any regulatory enforcement action or litigation, the regulator or private plaintiff will rely on the documentary 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, the company's 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," always thinking of what issues may come up in litigation and how to mitigate those 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. They ask 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 appropriately tailored cybersecurity governance practices and review the governance that clients already have in place. We advise on whether changes may be warranted to bring a client's governance in line with regulatory expectations and best practices.

Risk Assessment Analysis

Risk assessment is a fundamental building block, as well as a best practice, of cybersecurity planning. We work with clients to help identify and assess these risks, drawing on our wide range of expertise conducting such assessments from a legal perspective. This includes determining the company's most valuable assets, how they are protected and who can access that information. Where clients have already conducted such an assessment, we review and comment on their assessment to determine if it meets accepted practices.

Policies and Procedures

The Skadden Privacy and Cybersecurity Group has experience creating and reviewing all of the policies and procedures companies require, including external-facing security policies, internal policies guiding the use of 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.

Employee Training

A company's cybersecurity planning is only effective if employees are sensitized to the related risks through training. While companies generally design and implement such training internally, we work with clients to make sure that the scope and level of training would satisfy a regulatory inquiry and best protect the company if its practices were challenged in a litigation.

Insurance

Cyber insurance is a critical aspect of mitigating cybersecurity risk. Our insurance team works with clients to review existing policies to determine whether cyber insurance is warranted, help clients negotiate cyber insurance coverage and advise on the scope of coverage if an attack occurs.

Vendor Management Assessment

One of the most critical threat vectors that companies face is cyberattacks that exploit a third-party vendor's network connection to a company. We review clients' vendor management processes to determine if appropriate cybersecurity requirements are in place, and review third-party vendor agreements to determine if the client is adequately protected.

Cybersecurity and Privacy

Continued

Cybersecurity Rapid Response Services

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, they also must quickly manage an array of demands and pressures from the media, government officials, customers, business partners and shareholders. Companies also must be prepared for the reality that bloggers and the media can sometimes 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 want to be informed immediately. 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 and experience to help companies manage an attack and minimize legal exposure.

Forensics

The Skadden CRRT includes attorneys with technology and cybersecurity experience who can work with a client's forensic experts to evaluate the cyberattack, and determine the best way to approach remediation efforts. Skadden has 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

The CRRT stays up to date on all current state and federal data breach notification requirements. We can rapidly advise clients on whether disclosure to affected individuals is required and manage multistate notification processes.

Managing Public Disclosures

Skadden has a long history of helping clients make appropriate public statements during a crisis. In the case of a cyberattack, it is important to review all public statements to ensure that they are consistent with legal requirements and that they 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

The CRRT includes attorneys knowledgeable on SEC and regulatory rules, who 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. We also work with clients on any presentations or reports they need to make to regulators.

C-Suite and Board Support

Cyberattacks can quickly become C-Suite and board-level issues. CRRT members 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.

Litigation

Class action and shareholder derivative lawsuits are a reality following any cyberattack. The CRRT includes members of our Mass Torts, Insurance and Consumer Litigation Group, who can prepare the company for any type of class action lawsuits and defend against ensuing litigation.