Privacy, Data Protection, and Cybersecurity

Our Privacy, Data Protection, and Cybersecurity practice is guided by a team consisting of members with an extraordinary level of specialized knowledge and deep technical backgrounds in the fields directly related to this new and rapidly evolving practice area. And because we are also highly focused, experienced litigators, our group is uniquely positioned to identify the risks of a data breach, translate the technical issues into language that business people can understand, and suggest practical actions to minimize legal and criminal exposure.

The highly skilled individuals who drive this practice include a number of attorneys who are Certified Information Privacy Professionals in the United States (CIPP/US). Our team also includes partner Christopher Ott, a former cybercrimes prosecutor for the Department of Justice, who has a nationwide practice dealing with the exotic consequences of privacy issues, including criminal liability and thorny state and federal regulatory issues.

With our extensive technical and legal expertise, and an ability to develop compelling, effective approaches to data protection issues, we help clients both manage, and head off, regulatory inquiries, investigations, and actual litigation. This frequently means contending with a complex matrix of technologies, best practices, regulations, and statutes. In these situations, our job is to assist clients in determining which of these apply to them, and how to respond to questions of compliance, accountability, and risk control.

As data protection and cybersecurity affects virtually every business, we advise clients across a broad range of industries and technologies, including: artificial intelligence (AI)/machine learning, Internet of Things (IoT), high-end retail, cryptocurrency, bot mitigation, blockchain, fintech, bioinformatics, connected device technology, wearables, big data, computer science, trade associations, non-profits, adtech, and highly sophisticated biotech companies. Once we gain a thorough and detailed understanding of a client's business, we work across the entire data life cycle, from creation to processing, aggregation, and transmission.

Specifically, we help clients navigate current and pending privacy regulation, including the European Union's General Data Protection Regulation (GDPR) scheme and California's Consumer Privacy Act (CCPA), as well as more focused provisions, such as the Children's Online Privacy and Protection Act (COPPA), the Gramm-Leach-Bliley Act, and relevant Federal Trade Commission (FTC) rulings. We have also guided clients through the effects of lesser-known regulations, including the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM), the Fair Credit Reporting Act (FCRA), the Telephone Consumer Protection Act (TCPA), and other federal data breach laws.

Our work additionally includes assisting clients in reviewing, evaluating, and revising internal policies and data security requirements, to manage risk posed by both vendors and customers, from both a security and a compliance perspective. In this context, we place particular importance on the adoption of policies and procedures that reflect industry best practices. While regulation and law are still changing, best practices provide a (relatively) safe harbor from liability and risk. We work with clients to define it,

implement it, and regularly review it.

We emphasize a hands-on, business-oriented approach. We give clients workable, real-world guidance in the legal implications of data-related issues. We see our role as providing them with specific, applicable recommendations, as well as assisting them in foreseeing potential issues, all provided in the context of their specific business goals. Even cutting-edge, technology-oriented companies are often unaware of the risks and potential liabilities embedded in their everyday operations. We help them daylight it, and manage it.