Privacy, Cyber & Data Governance

Wiley Rein’s Privacy, Cyber & Data Governance team is deep and broad. Our attorneys, many of whom are IAPP-certified, are involved in developing privacy regulations and public policy including and beyond HIPAA, in industries from high tech to government contractors to fintech to brick-and-mortar retailers. We cover a range of challenges and are trusted advisors to companies and associations working on privacy and data security around the world, advocating here and abroad for sensible regulation.

The firm advises clients across the spectrum of emerging data security and privacy laws, covering requirements in the health care, telecommunications, government contracting, and financial services industries (as well as vendors to these industries), and the several statutes administered by the Federal Trade Commission (FTC). We are involved at the National Institute of Standards and Technology (NIST), shaping privacy engineering, cybersecurity, and Internet of Things (IoT) best practices. We also are working on key national security issues raised by data access and governance, particularly by foreign actors and investors. This can involve advice on surveillance, encryption, and shifting expectations.

We advise clients on state cybersecurity and privacy laws, including online privacy legislation, automated vehicle legislation, and state breach notification legislation, among others. Recently, the firm has been working with the California Consumer Privacy Act (CCPA) and California’s new IoT cybersecurity law, providing analysis and strategic counsel for multiple clients. We have an associate effectively acting as in-house counsel to a major client on state privacy law, and another colleague who manages major data breaches and incidents for government contractors. We help companies comply with New York Department of Financial Services Cybersecurity Regulations, the Illinois Biometric Information Protection Act, and myriad other requirements.

We help clients assess the landscape in Europe, Asia, North America, Australia, Latin America, and the Middle East concerning forced localization requirements for communications networks and “cloud” storage; privacy, data protection, and information security; law enforcement assistance, data retention, and lawful interception; and telecommunications and Internet regulation. We navigate ambiguous international requirements and help find workable solutions to sometimes conflicting requirements. We advise clients on the EU General Data Protection Regulation (GDPR), conducting internal audits and helping to bring practices into compliance, including...
implementing best practices for data retention, revising privacy policies, and managing vendor agreements. We also assist clients in navigating the Privacy Shield certification process to allow for the transfer of personal data from the EU.

Our team is comprised of many professionals who meet clients' needs and help anticipate regulatory challenges. They address various regulations, enforcement contexts, and litigation issues, across sectors and federal agencies, many with specialized backgrounds in fintech, emerging technologies, telecom regulation, health care, Internet security, wireless technologies, cybersquatting, and national security.

Representative clients include Tier 1 wireless providers and ISPs, major government contractors, innovators in the Internet of Things and machine learning, and more. We help global satellite companies, health care providers and insurers, North American transportation leaders, computer science and information technology companies, technology and application innovators, global Internet retailers and cloud service providers, national and global trade associations, and other Fortune 500 companies tackle the full spectrum of privacy and security issues.

Representative **Privacy** projects include:

- Advising on compliance, risk management, and business strategy, from data governance to new product and service offerings.
- Adapting available options for maintaining a free flow of personal information to a company's needs and risk exposure.
- Developing and implementing privacy and security policies consistent with applicable law and business objectives.
- Identifying solutions to the challenges raised by cross-border data flows.
- Conducting compliance and due diligence investigations for acquisitions and investments.
- Negotiating and drafting vendor contracts.
- Assisting in litigation and enforcement matters.
- Monitoring developments in privacy law worldwide and advocating policy positions in the U.S. Congress and key national and international regulatory agencies.

Representative **Cyber & Data Governance** projects include:

- Developing policies and procedures to help technology companies, critical infrastructure owners, business associations, nonprofits, defense contractors, and others manage cyber risks, including incident response plans and governance structures. We also advise Boards of Directors.
- Responding to congressional and agency investigations into security issues and vulnerabilities.
- Anticipating and shaping activity across the federal government (NTIA, NIST, FTC, DOJ, FCC, DHS, and the White House) involving cyber initiatives that directly and indirectly impact companies. This includes the Cybersecurity Information Sharing Act of 2015; several Executive Orders; the NIST *Framework for Improving Critical Infrastructure Cybersecurity*; NIST publications; proceedings on botnets, market transparency, and the security of the communications and Internet infrastructure.
- Advising government contractors on contractual and regulatory information security requirements, cyber incident reporting obligations, and information system audit best practices.
Advising clients on all aspects of successfully implementing new cybersecurity requirements for federal contractors, including DFARS 252.204-7012, Safeguarding Covered Defense Information, including:

- Interpreting and applying NIST 800-171 security controls for contractor systems.
- Evaluating contractors’ information systems and applicability of regulation to same.
- Assisting in corporate gap analyses and shaping compliance strategies.

Engaging with agency customers to coordinate FISMA audits of contractor information systems, including negotiations involving the scope of audits and any potentially malicious penetration testing.

Interfacing with CFIUS and “Team Telecom” to help clients with transactions involving foreign ownership, as well as national security compliance under mitigation and network security agreements.

Incident handling and management, including mandatory and voluntary disclosures of cyber incidents to customers, regulators, and federal agency purchasers.

- We collaborate with law enforcement to identify and investigate criminal hackers.
- We oversee computer forensic investigations to understand how a cyber incident occurred, evaluate the scope of the incident, and determine attribution.

Managing vulnerability assessments, penetration testing, and third-party security vendors to maximize privilege and assist in remediation planning.

Helping companies interact with the U.S. Department of Homeland Security (DHS) to share information and assess risks to business operations and critical infrastructure. This includes communications protected by the Cybersecurity Information Sharing Act of 2015 and the Protected Critical Infrastructure Information (PCII) program.

Negotiating contractual language for cybersecurity and data security obligations and indemnifications.

Assisting ISPs, telecoms, and other technology companies in responding to law enforcement requests for data and complying with the requirements of the Electronic Communications Privacy Act.

Litigating dozens of matters involving cybersecurity and computer forensic evidentiary issues, including False Claims Act and Computer Fraud & Abuse Act cases. When needed, we have combined our litigation skills and government contracting background to handle cyber-related litigation. This includes cybersquatting litigation to end domain-name hijacking and other exploitations.

Advising on the legality and risks of certain defensive and offensive measures, as well as federal policy on “hacking back,” and on the implementation of vulnerability disclosure programs or “bug bounty” programs.

With many professionals maintaining clearances, we are prepared to help organizations with any aspect of a cybersecurity challenge.

Contact Us

Megan L. Brown
202.719.7579 | mbrown@wileyrein.com
Privacy, Cyber & Data Governance Continued

Matthew J. Gardner
202.719.4108 | mgardner@wileyrein.com

Dorthula H. Powell-Woodson
202.719.7150 | dpowell-woodson@wileyrein.com