wiley

Privacy, Cyber & Data Governance

From the high-tech sector 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.

Wiley's Privacy, Cyber & Data Governance team assists clients with a full spectrum of privacy, cybersecurity, and data governance issues, from compliance to transactional diligence to investigations, enforcement, and litigation. We have an exceptionally wide range and depth of experience in privacy and cyber matters across sectors, including tech, telecom, health care, government contracting, and financial services. Our practice spans federal, state, and international levels, featuring IAPP-certified attorneys and numerous former government officials, and we routinely advocate for sensible privacy and cyber approaches before government agencies.

Our practice has a particular expertise in privacy and cybersecurity issues involving cutting-edge technology and data use, including novel health care applications and regulatory approaches and best practices for artificial intelligence (AI). It also includes work on key national security issues raised by data access, particularly by foreign actors and investors, advice on surveillance and encryption, and responses to ransomware attacks and other cybersecurity incidents. We also have a unique practice assisting investors and acquirers in conducting privacy, cybersecurity, and regulatory due diligence in proposed transactions, working hand in hand with deal counsel.

At the federal level, we have deep experience with key agencies working in privacy and cybersecurity. This includes the Federal Trade Commission (FTC), National Institute of Standards and Technology (NIST), Department of Health and Human Services (HHS), Department of Homeland Security (DHS), and Department of Commerce. We closely monitor state law developments, including in California, Virginia, and Colorado, as well as the Illinois Biometric Information Privacy Act (BIPA), and have experience dealing with State Attorneys

Capabilities

- Artificial Intelligence (AI)
- Connected & Autonomous Vehicles
- Cyber and Privacy Investigations, Incidents & Enforcement
- Cyber Insurance
- Digital Assets, Cryptocurrencies, and Blockchain
- Digital Health
- GDPR and Global Privacy
- State Privacy Laws
- Transactional Support and Due Diligence on Privacy and Cybersecurity

General.

We also advise clients on privacy and data regulations in Europe, Asia, North America, Australia, Latin America, and the Middle East and work closely with local counsel in those regions to deliver full-service counseling. Our expertise includes advising on cross-border data transfers, forced localization requirements for communications networks and "cloud" storage; law enforcement assistance, data retention, and lawful interception; and telecommunications and internet regulation. 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 assist clients in navigating cross-border data transfers from the EU, including implementing standard contractual clauses and other approaches in light of the *Schrems II* decision. We navigate ambiguous international requirements and help find workable solutions to sometimes conflicting requirements.

Representative **Privacy** matters include:

- Developing and implementing privacy and security policies in accord with applicable law and business objectives.
- Conducting compliance and due diligence investigations for acquisitions and investments.
- Representing clients in regulatory investigations and litigation.
- Identifying and implementing solutions to challenges raised by cross-border data flows.
- Advising on company-wide compliance, risk management, and business strategy on privacy and data governance.
- Advising companies on compliance with state laws including New York Department of Financial Services Cybersecurity Regulations, the Illinois Biometric Information Protection Act, and the California Consumer Privacy Act (CCPA).
- Negotiating and drafting vendor contracts.

Representative **Cybersecurity** matters 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.
  - Drafting System Security Plans and Plans of Action and Milestones for addressing gaps.
  - 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 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.

Key Contacts

Megan L. Brown
Partner
mbrown@wiley.law
202.719.7579

Duane C. Pozza
Partner
dpozza@wiley.law
202.719.4533