wiley

Cyber and Privacy Investigations, Incidents & Enforcement

Wiley's team is extensively prepared to handle every aspect of a security incident or vulnerability from assessing risk, managing reputational damage, compliance obligations, communicating with federal and state law enforcement, and litigation. We are former senior officials from the U.S. Department of Justice, Federal Bureau of Investigation (FBI), Federal Communications Commission (FCC), and Federal Trade Commission (FTC), as well as attorneys who have earned the designation of Certified Information Privacy Professional (e.g., CIPP/US, CIPM).

We provide comprehensive counsel on cutting-edge legal, policy, and technical issues involving cybersecurity and privacy across a variety of sectors including telecommunications, government contracting, health care, financial services, and aviation or transportation. We are extensively involved with the National Institute of Standards and Technology (NIST) and other federal government policy making bodies working on key national security issues raised by cybersecurity, data access, and data governance concerns, particularly related to foreign actors or investors.

Our attorneys are deeply involved in developing national cyber or privacy policies and regulations including compliance with the new Cyber Incident Reporting for Critical Infrastructure Act of 2022. We advise a variety of corporate clients and trade associations as the U.S. Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA) proposes rules for reporting significant cybersecurity incidents or ransomware payments.

Our cybersecurity clients seek our advice for three phases of cybersecurity legal needs:

1. Preparing cybersecurity incident response plans and related policies in advance of a cyber incident or ransomware attack;
2. Serving as "breach coaches" during a cybersecurity event, including notification of DHS/CISA, law enforcement or relevant regulatory agencies, coordination with forensic services, communications consultants, or third party vendors; and
3. Defending against any subsequent enforcement actions or litigation.

Our privacy clients look to us for guidance on domestic and international data access and data governance issues frequently involving data protection, information security, records retention, E-commerce, intellectual property, or consumer protection. We have extensive experience in handling regulatory issues before the FCC or the FTC. We advise on long-standing federal standards such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), the Fair Credit Reporting Act, and the Gramm-Leach-Bliley Act as well as emerging state standards.

Our services include:

Cybersecurity and Privacy Compliance and Risk Management

- Build full-scale compliance programs for domestic and international operations, including:
  - Data mapping and risk assessment
  - Data subject access request management policies, procedures, and workflows
  - Cybersecurity vulnerability and gap assessments
  - Review and update contracts and agreements to reflect data privacy obligations and data processing practices
  - Privacy and security compliance for new product and service development and advertising, including under state regulation of Internet of Things (IoT) security laws
- Supervise third party consultants in audits and gap assessments, often conducted at the direction of counsel to aid in compliance and prepare for litigation.
- Update data privacy and information security policies, procedures, and programs for businesses with both domestic and international operations.
- Advise on compliance with contractual and regulatory requirements ranging from DFARS 252.204-7012 clause to evolving prohibitions on the use of certain vendor equipment.
- Coordinate notification to law enforcement, DHS/CISA, and other agencies of data breaches, significant cyber incidents, or ransomware payments as appropriate.
- Advise and negotiate consensual FBI monitoring, government cyber assessments, and other collaborations with government.

Policy Planning and Advocacy

- Provide legal counsel and to corporate leadership on new legal and regulatory requirements in cyber and privacy.
- Monitor and assess the potential impact of emerging technologies on law, regulations, and/or policies.
- Represent clients in virtually all major federal and state regulatory proceedings on cyber and privacy from rulemakings publications by the NIST.

Critical Infrastructure Protection

- Advice on emerging legal, regulatory, and policy obligations related to critical infrastructure cybersecurity.
- Develop comprehensive critical infrastructure protection plans and assist in information sharing on threats and vulnerabilities.
- Advise on emerging incident reporting rules at DHS, compliance with Security Directives from sector specific agencies, and related efforts to address critical infrastructure.

Data Breach, Incident Response, and Incident Reporting

- Help clients prepare for, and respond to, data breaches and the full range of government investigations they may prompt.
- Provide immediate support and rapid response, for clients that learn of a possible data breach or cyber incident.
- Develop and test comprehensive cybersecurity incident response plans that address internal and external actions to take in the wake of a data security incident.
- Assist companies in notifying regulators and third parties and managing crisis communications.
- Represent clients in all forms of litigation associated with data breaches and other security incidents.

Enforcement Actions or Regulatory Inquiries

- Represent clients in FCC enforcement actions under the Communications Act involving CPNI regulations and reporting, among other requirements.
- Represent clients in FTC enforcement actions alleging fraud or deceptive and unfair business practices related to privacy and cybersecurity practices.
- Represent clients in SEC enforcement actions concerning alleged insider trading, misleading disclosures, or other securities irregularities or accounting deficiencies.
- Represent clients in Inspector General (IG) and U.S. Department of Defense (DoD) reviews related to cybersecurity and incident reporting.
- Handle multi-jurisdictional oversight and enforcement actions and coordination of litigation.
- Manage formal and informal Congressional inquiries related to diverse cybersecurity and privacy issues.

Employee Privacy and Cyber Issues

- Advise on the full range of employment-related issues impacted by privacy and cyber risk management, from insider threat programs to helping obtain security clearances.

- Counsel clients on compliance with the Fair Credit Reporting Act and analogous state laws regarding pre-employment background checks and post-hire investigations.
- Counsel businesses on privacy issues related to work-from-home and COVID-19.
- Work with companies whose employees or customers are facing targeted, sophisticated phishing campaigns, including spoofing attempts and suspected email compromises.
- Represent and protect companies and their employees who are victims of online harassment, including nonconsensual pornography, cyber stalking, reputation attacks, identity theft, and other forms of digital abuse.
- Our work can include support of the company's investigations into these matters, packaging the evidence for cooperation with law enforcement, and protection of corporate intellectual property, particularly as to domain name abuse. More information on our cybersquatting capabilities can be found here.

Law Enforcement Access and Judicial Process Compliance

- Provide advice on compliance with search warrants, subpoenas, "2703(d) Orders" for digital evidence or computer media, including geo-fence warrants. This includes building compliance programs for handling legal process and to meet the obligations of the Communications Assistance for Law Enforcement Act (CALEA).
- Advise clients on the applicability of the Computer Fraud and Abuse Act to commercial and online activities, including social network sites and IP protection.
- Advise on cyber defensive operations and services, under the Cybersecurity Information Sharing Act of 2015 and other laws.
- Coordinate threat briefings with federal law enforcement and homeland security officials.

Privacy and Cybersecurity Trainings

- Provide privacy training options to businesses of all sizes in privacy readiness and compliance, including trainings to meet compliance requirements for the California Consumer Protection Act (CCPA), General Data Protection Regulation (GDPR), HIPAA, the Privacy Act, and EU data authority guidance.
- Plan and conduct tabletop exercises with companies at the tactical and Board levels to simulate an event built around the company's risk profile, often partnering with inside or outside forensic experts and media relations professionals.

Subscribe here to receive real-time in-depth updates with key information to stay ahead of privacy and cybersecurity developments, including a monthly report on developments in privacy and information security law. You will also receive information on upcoming privacy and cyber-related events.