
Data Security

Cybersecurity and Privacy

We have advised many of the world's most sophisticated companies on sensitive investigations and forensics related to data breaches, regulatory requirements and enforcement at the federal, state and international levels, compliance, public policy developments, congressional, state attorney general and regulatory investigations, incident planning, critical infrastructure protection, and interaction with law enforcement, as well as a variety of other data security issues.

Our lawyers have a wide range of litigation, regulatory and corporate experience, and the team includes many who have held senior positions at the Central Intelligence Agency (CIA), and the Departments of Justice (DOJ), Defense (DOD) and other key departments. For example, former Deputy Attorney General Jamie Gorelick has deep experience counseling clients on cybersecurity and is a member of DOD's Policy Board, and Benjamin Powell served as general counsel to the first three directors of National Intelligence and helped design and implement compliance and oversight mechanisms related to privacy and cybersecurity. The team also includes Stephen Preston, a former general counsel of both the CIA and the DOD, and Aaron Zebley, a former federal prosecutor with more than 18 years of DOJ experience who served as deputy special counsel under Special Counsel Robert Mueller during the investigation into Russian interference in the 2016 US presidential election.

Areas of Focus

Data Breaches

WilmerHale's Cybersecurity Practice has helped dozens of clients with every aspect of data breach incident preparation, response and recovery. We regularly counsel companies responding to data breaches about state, federal and international breach notification requirements, SEC and other regulatory obligations, contractual reviews, litigation exposure, liaison with government agencies, media inquiries, and compliance improvement efforts. In response to serious breaches, WilmerHale lawyers have assisted companies by overseeing internal investigations and engaging outside forensic experts as well as assisting with incident

management and response planning to prepare for the possibility of data breaches.

Representative matters include:

- Regularly assisting companies in complying with data-breach reporting obligations across the states as well as under sector-specific federal regimes, such as the Health Insurance Portability and Accountability Act and the Gramm-Leach-Bliley Act and their implementing regulations
- Completing sensitive internal investigations for boards of directors and senior management of network breaches to provide advice on corporate notification, disclosure, and other remedial requirements
- Helping the largest technology companies in the country interact with US government agencies in response to network breaches
- Assisting major energy utilities respond to law enforcement and other government requests related to cybersecurity incidents
- Assisting multiple commercial companies and defense contractors responding to Advanced Persistent Threats discovered within their networks
- Leading internal investigations related to improper conduct of employees resulting in data and network breaches
- Assisting an international bank in seeking removal of information stolen by a hacker and uploaded to a file-sharing site in the United States
- Assisting a national corporation with breach notification obligations in connection with its contractor's improper disclosure of retiree health information

Compliance Counseling and Regulatory Investigations

Rapidly changing data security threats and rapidly shifting regulatory obligations mean that companies need to address their data security posture before they face a breach. WilmerHale assists companies in assessing their regulatory obligations and data security needs, advising corporate boards about data security, putting in place effective information security programs, incident management and response planning, ensuring compliance with corporate governance and related obligations, and responding to regulatory inquiries that arise with increasing frequency from, among others, the Federal Trade Commission (FTC), sector-specific regulators, such as the Securities and Exchange Commission, the financial regulators that make up the Federal Financial Institutions Examination Council, the Federal Energy Regulatory Commission, and others.

Representative matters include:

- Representing one of the world's largest technology companies in an extensive FTC investigation of its data security practices related to development of consumer software
- Assisting numerous technology, e-commerce, financial services, defense and electronic equipment companies in development of data security policies and procedures

- Advising numerous companies on the requirements of federal, state and foreign data security laws, such as the USA PATRIOT Act, Foreign Intelligence Surveillance Act, Computer Fraud and Abuse Act, Electronic Communications Privacy Act, Stored Communications Act, and their state equivalents
- Advising numerous providers of cybersecurity services on possible legal risks involved in various activities designed to detect cyberthreats
- Advising numerous companies on incident management and planning to prepare for possible breaches
- Assisting major technology companies in responding to state attorney general and federal inspector general investigations
- Assisting defense contractors in assessing their obligations under Department of Homeland Security and Defense Department cyber threat information-sharing programs
- Regularly undertaking due diligence on mergers and acquisitions related to cybersecurity and data protection, including drafting model provisions for corporate transaction agreements
- Advising a major national bank on legal and regulatory concerns raised by surveillance and information-sharing for cybersecurity purposes
- Helping numerous companies obtain Safe Harbor certification, and in structuring international flows of personal data to achieve compliance with legal requirements
- Assisting companies in complying with PCI-DSS obligations

Government Contracting

Companies that provide goods and services to federal, state and local governments are increasingly subject to special data security obligations, while at the same time the movement of government agencies to reliance on cloud services has opened up new opportunities for cloud and cybersecurity service providers.

Representative matters include:

- Assisting a major financial institution in negotiating the data security and data-sharing arrangements under a contract with the Department of Housing and Urban Development
- Counseling cloud computing clients on the requirements for the FedRAMP and the Cloud Credential Exchange programs
- Advising defense industrial base companies on their obligations under proposed Federal Acquisition Regulation changes to data-breach reporting requirements

Public Policy and Congressional Investigations

Legislatures and regulatory agencies across the United States and around the globe are increasingly investigating data security issues and debating new requirements. WilmerHale

has assisted dozens of clients in responding to these inquiries and helping to shape these debates.

Representative matters include:

- Advising numerous companies on responding in the United States and internationally to issues created by the recent disclosures of US intelligence programs involving the acquisition of data by governments under a variety of authorities
- Helping a major data brokerage company respond to congressional inquiries
- Advising a major automobile company on responding to congressional inquiries related to privacy and cybersecurity
- Serving as outside counsel for the cybersecurity task force of a large banking association
- Assisting a major technology company in addressing possible reform of the Computer Fraud and Abuse Act
- Advising numerous large technology companies, including those providing significant consumer services, defense services and other commercial companies

Litigation

Data security issues are increasingly winding up in the courts, whether through consumer class actions, government enforcement efforts, challenges to government surveillance programs or fights over insurance coverage.

Representative matters include:

- Representing a major internet service provider in class action litigation arising from improper release of consumer information
- Representing a major social networking company in litigation before the Foreign Intelligence Surveillance Court
- Representing a major broadband and telecommunications company in litigation over the National Security Agency's surveillance programs
- Advising a major bank about litigation options for responding to data thieves in the United States and Europe
- Assisting a software company in responding to claims under the Computer Fraud and Abuse Act

The European Union, China and Other Non-US Jurisdictions

Data security is a global issue. With offices in Brussels, Frankfurt, London, Berlin and Beijing, we regularly assist companies in navigating the often complicated and inconsistent regulatory regimes they face in operating in many jurisdictions.

Representative matters include:

- Advising a major cloud computing company on the data security regulations applicable to the financial sector in the European Union, many of its member states, China and numerous other jurisdictions around the world
- Advising numerous companies in sectors across the economy about safeguarding information resources consistent with data protection regulations on six continents
- Advising numerous companies about legal and policy implications of reforms to the EU data protection law, as well as new European and national initiatives regarding network security and cybercrime
- Advising a leading cloud services provider on a draft industry code of conduct for data security and data privacy
- Advising a US company on responses to data security breaches in its China subsidiary
- Advising multiple US and non-US companies on compliance with Chinese state secrets regulations

Key Contacts



Benjamin A. Powell

PARTNER

✉ benjamin.powell@wilmerhale.com

📍 WASHINGTON DC

☎ + 1 202 663 6770



Kirk J. Nahra

PARTNER

✉ kirk.nahra@wilmerhale.com

📍 WASHINGTON DC

☎ + 1 202 663 6128



Dr. Martin Braun

PARTNER

✉ martin.braun@wilmerhale.com

📍 FRANKFURT ☎ + 49 69 27 10 78 207

📍 BRUSSELS ☎ + 32 2 285 49 00



Jason C. Chipman

PARTNER

✉ jason.chipman@wilmerhale.com

📍 WASHINGTON DC

☎ + 1 202 663 6195