Cybersecurity and Data Privacy

Section Chair
Calvin B. “Cal” Marshall, Jr.
D. 423.757.0214
E. cmarshall@chamblisslaw.com

As cyber threats and compliance regulations exponentially increase, the Chambliss cybersecurity and data privacy team remains a trusted resource for risk identification, compliance, data breach response, cyber insurance policy review, and other related matters.

With the vast amounts of data that businesses hold today, maintaining cybersecurity and data privacy is of paramount importance. We assist our clients with everything from identifying legal obligations in this space to implementing GDPR compliance measures to managing and responding to cyberattacks, including those that involve data breaches. We realize that when it comes to cybersecurity and data privacy, a one-size-fits-all approach is not the answer. Our team collaborates with clients to identify how we can tailor solutions to fit their individual business models and goals.

What We See on the Horizon

- **There are increasing cyberattacks on a variety of industries, including those that can threaten an organization’s very survival.** We help clients better understand current cyber risks, measures needed to address those risks, including the “human element” of cyber risk, and we help clients respond to and recover from cyberattacks when they occur, including evaluation and management of legal breach reporting obligations.

- **As technology continues to advance, as risks grow, and as data privacy and security laws evolve, clients need to make sure they have**

Related Services

- Chambliss Startup Group
- Financial Services
- Mergers and Acquisitions
- Software, Website, and Domain Names
- Trade Secrets
- eHealth, Data Privacy, and Security

Related Industries

- Aviation
- Electronic, Medical, and Other Devices
- Health and Wellness
- Information Technology
- Manufacturing
- Media, Publishing, and Entertainment
- Software
- Startups and Emerging Companies

Related People

- Calvin B. “Cal” Marshall, Jr.
- William P. Aiken
- Lisa M. Kiner
- Eric J. Stocking

up-to-date safeguards, compliance measures, and training. Our attorneys assist clients in identifying and implementing both required and "best practice" cybersecurity and data privacy measures.

- **The costs of cyberattacks and data breaches continue to increase, and these costs are often much greater than a particular organization would expect.** Our attorneys serve as trusted advisers to minimize these data risks and associated costs, allowing clients to focus on running their businesses in secure environments without undue disruption.

- **Even as technological advances allow companies to be more nimble, mobile, targeted, and efficient, they have made businesses of all sizes vulnerable to cyberattacks like never before**. And, cyberattacks have become more sophisticated and wide-ranging, adversely affecting businesses as diverse as mom-and-pop corner groceries and international shipping giants. It's important that all companies, no matter the size, have data breach response plans in place.

A Snapshot of Our Depth

- Current and changing data regulations
- Cybersecurity risks and protocols
- Incident response plans
- Cyberattacks
- Cyber-related disputes and litigation
- Privacy and data security issues in mergers, acquisitions, or joint ventures
- Cyber insurance coverage

Experience

Advised clients regarding compliance with HIPAA, 42 CFR Part 2 (Substance Abuse Confidentiality Regulations), the California Consumer Privacy Act, and other federal and state privacy, security, and breach notification laws

Advised businesses on consumer data collection and privacy disclosures, including EU GDPR compliance

Assisted clients in responding to ransomware and other data security incidents, including identification of legal obligations and management of data breach response processes and communications

Advised clients regarding a wide variety of other potential breach incidents, including lost files, misdirected e-mails, physical facility security incidents, and other issues

Counseled health care and other clients regarding privacy, security, and cyber risks and questions, including analysis of data flows, in creation and negotiation

of contracts with their clients, vetting and negotiation of arrangements with their vendors, and in merger and acquisition-related due diligence

Created, evaluated and/or revised compliance programs and policies on behalf of clients