Privacy

Privacy, Cybersecurity, and Data Breaches

Businesses large and small are becoming increasingly data driven. The vast amounts of data collected every minute of every day give businesses increased opportunities – and increased responsibility.

The law and policy surrounding data privacy and cybersecurity are constantly developing as existing technology continues to evolve and new technology emerges. Business owners, service providers and government officials have to balance the exciting opportunities that artificial intelligence, the Internet of Things, wearables, cloud computing and any number of other technologies provide with the responsibility to protect the privacy of individual persons and business partners. Brooks Pierce has long been established in this ever-changing area of law. We counsel executives and businesses in a wide variety of industries on developing privacy policies, remaining compliant with state and federal regulations, consumer protection matters, information security and risk mitigation practices. Some of the industries we counsel include:

- **IT** – We advise companies on the growth of technology and establishing network privacy and security
- **Healthcare** – We counsel healthcare providers regarding HIPAA law, the use of patient information, and electronic Protected Health Information (PHI)
- **Financial services** – We advise banks and other financial institutions regarding the Right to Financial Privacy Act and other financial privacy regulations and best practices to protect consumer information
- **Retailers** – We work with retailers to ensure that how they collect, transmit, store, use and manage large amounts of customer data is compliant with the ever growing set of laws that apply to their operations, including, for example, the CAN-SPAM Act and the Telephone Consumer Protection Act (TCPA)

Some of the digital privacy issues Brooks Pierce attorneys regularly advise companies on include:

Data Collection and Privacy Policies. A collection of federal, state and international laws govern how businesses collect, use, share and store data, both online and offline. Many of these laws address specific types of consumer data, including children's data (the Children's Online Privacy Protection Act), financial information (Graham-Leach-Bliley Act and the Fair Credit Reporting Act) and personal health information (HIPAA). Others such as the California Consumer Protection Act (CCPA) or Virginia Consumer Data Protection Act only apply when a business serves consumers located in certain regions. As a result of this patchwork quilt of laws, privacy compliance is not "one

size fits all"—particularly where costs and resource utilization are a factor. We work with businesses to create a privacy program that is unique to their needs.

Cyber Insurance and Vendor Agreements. Given the legal risks with online marketing and privacy, many insurers are offering data breach policies, but you need to be sure that they are sufficient to cover your potential risk and appropriate for your particular circumstances. We also regularly review third-party vendor agreements to determine whether they provide adequate compliance assurances and impose reasonable notification obligations in the event of a cyber incident.

Data Breach Response. When data breaches occur, business have a host of obligations to consumers, vendors, state and federal regulators. All 50 states have data breach notification laws, and HIPAA and Gramm-Leach-Bliley have their own notification rules. The costs of complying with notification laws, repairing the data breach, and restoring the reputation of your business's brand can be enormous. Having counsel engaged before a breach happens is the best way to mitigate those costs when problems do arise.

Cybersecurity. With the continuous changes in internet regulation, laws and guidelines, it can be difficult to keep up with the evolving needs of safety and security. Brooks Pierce can help identify and assess cyber risks from a legal perspective. We provide counsel on cybersecurity preparedness and assist clients by conducting cybersecurity assessments and by creating and reviewing incident response plans and written information security programs.

How can we help your business provide responsible security?

PEOPLE

Forrest Campbell Jr.

J. Benjamin Davis

Micole Little

Claire O'Brien

Mark J. Prak

Will Quick

Elizabeth Spainhour

Bryan Starrett

Marcus Trathen

Thomas G. Varnum

Will (Otis) Walker

Edwin L. West III

NEWSROOM

News

Will Quick Discusses Privacy & Cybersecurity Best Practices in Business North Carolina Feature
11.14.2022

Brooks Pierce Recieves 41 Tier-One Rankings in 2023 "Best Lawyers"
11.03.2022

Brooks Pierce Partner Discusses Data Privacy and Cybersecurity with *Business North Carolina*
Business North Carolina, 11.08.2021

Brooks Pierce Partner Named Chair of North Carolina Bar Association Young Lawyers Division
06.29.2021

Will Quick Named Vice-Chair of North Carolina Bar Association's Privacy & Data Security Section Council
06.21.2021

Events

Brooks Pierce Hosts Webinar on Data Privacy Law
07.14.2022

Will Quick Participates in Panel Discussion on Incident Response
05.07.2021

Brooks Pierce Partners Discuss Cybersecurity at NCTA Event
04.16.2015

Spainhour and Hartzell Present to Triad's Largest PR Association
03.10.2015

Publications

Key Takeaways from the IAPP Global Privacy Summit 2022

*NCBarBlog.com*05.12.2022

COVID's Long-Term Impact: Six Unique Legal Issues Facing Businesses in 2022
03.08.2022

Rethinking Your Cyber Insurance Needs as Your Workplace Evolves
Digital Media and Data Privacy Law Blog, 01.28.2022

Data Breach Defense for Educational Institutions
Digital Media and Data Privacy Law Blog, 06.16.2021

Brooks Pierce Capital Dispatch: Updates from the NC General Assembly and Governor's Office, May 14, 2021
05.14.2021