FENNEMORE.

Privacy and Data Security

Our privacy and data security practice addresses the administrative, regulatory and litigation concerns of businesses facing mounting threats and increasing state and federal regulation in the areas of data privacy, data breach and cybersecurity.

Our privacy and data security practice focuses on prevention and risk counseling, data breach prevention, cybersecurity incident investigation and response, regulatory compliance, privacy and data security policies and training, and related litigation and dispute resolution. Should a data breach, government investigation or litigation occur, our attorneys are prepared to work with clients to navigate the complex regulatory landscape of today's digital and in-person environment.

WHAT WE DO

We regularly work with clients who are doing business in person and online. Whether the need is developing compliant privacy policies or internal processes, responding to a privacy breach incident or responding to a cease and desist demand involving breach incident, our team will provide a valuable, cost-effective solution. The attorneys in this group work closely with clients facing the uncertainties created by the rapidly evolving law regarding consumer privacy. We routinely prepare privacy policies, data processing agreement, terms of use, and other agreements. We can also assist clients engaged in the business of online marketing and advertising, such as holding online sweepstakes and contests.

We work for you.

In the constantly changing consumer privacy landscape, we put our experienced attorneys to work on behalf of your evolving business.

We provide counsel and representation in the following areas:

- Privacy statutes, rules and regulations, including the California Consumer Privacy Act (CCPA) and other state consumer privacy laws, the Americans with Disabilities Act Amendments Act (ADAAA), California Online Privacy Protection Act, CAN-SPAM Act, Children's Online Privacy Protection Act (COPPA), Fair and Accurate Credit Transactions Act (FACTA), Fair Credit Reporting Act (FCRA), Federal Identity Theft Assumption and Deterrence Act (ITADA), Genetic Information Nondiscrimination Act (GINA), Electronic Communication and Privacy Act (ECPA), Payment Card Industry Data Security Standards (PCI DSS and PA-DSS) and Telephone Consumer Protection Act (TCPA)

- Health care regulations and reporting, including the Health Information Technology for Economic and Clinical Health Act (HITECH) and the Health Insurance Portability and Accountability Act (HIPAA)

- Document retention requirements, information sharing and information disclosure

- Management and employee training regarding data security and privacy requirements and development of applicable policies and procedures

- Internal investigations, permissible monitoring of employees, and background checks

- Government investigations (preparation and response)

- Litigation related to privacy and data security incidents or breaches

- Online copyright and ISP safe harbors under the Digital Millennium Copyright Act (DMCA)

- Contract negotiation involving data security and privacy matters

- Privacy and security provisions for cloud, data center, and network infrastructure provider agreements, including the Stored Communications Act (SCA) and the Wiretap and Stored Communications Acts

- Anti-cybersquatting, domain name strategies and trademark issues (ACPA, UDRP, URS)

- Data and security breaches

- Online speech and conduct (CDA and ISP terms of use) and social media issues

- Website hosting agreements, terms and conditions of use, and privacy policies, as well as clickwrap and browse-wrap license agreements