

Data Privacy

According to statistics provided by the Data Breach Level Index, hackers and thieves are stealing more than 227,000 personal records per hour as of 2017, generally targeting customer information for purposes of identity theft. Furthermore, more than half of all enterprises will suffer at least some kind of data breach in any given year.

The damages - in terms of reputation, lost customers, and costs of investigation and remediation - typically run between \$50,000 and \$170,000 per 1,000 records, based on surveys done by respected companies such as Verizon and Kroll; and those costs do not include potentially significant fines, penalties, and judgments incurred on account of liability to third-parties.

The potential for a breach or inadvertent release of data exists every time personally identifiable information is gathered, regardless of the size or financial health of your business. Collecting, storing and using data effectively while protecting the privacy of individuals is a critical challenge facing all businesses.

If you can't answer "yes" to the following questions, then you are not using "best practices" for information security protocols, and should consider seeking help, which we can provide:

1. Does your company have a Written Information Security Program?
2. Has your company appointed a Security Officer?
3. Does your company require that all email containing personal private information be encrypted, and that all portable devices (laptops, phones, thumb drives, etc.) be encrypted while in use and while at rest?
4. If your vendors have access to private personal information that you collect and store, do you have protections in place to reduce or eliminate exposures from unauthorized access to that information by a third party?

Our team of lawyers knows how to help clients defend against, prosecute and respond to data privacy breaches. In recent years, interviewees of Chambers USA have described our litigators as "a strong group with extensive trial skills" which is "dedicated to client service," and one which has a "deep bench in its Boston office."

Our Clients

We regularly assist clients in proactively addressing data, privacy and cybersecurity matters that arise out of the misuse, or potential misuse, of sensitive personal information. Our clients include financial service companies, healthcare providers, restaurant and hospitality groups, retailers, and telecommunications and technology companies. We have provided services to e-commerce

companies engaged in online media, software-as-a-service, educational service and other activities. Clients involved in various real estate enterprises turn to us as well for risk management assessment and data security advice.

What We Do / Our Experience

Privacy laws are continually evolving, vary by jurisdiction, and are enforced by federal and state regulators and authorities at different levels. Our attorneys help clients with a full range of data, privacy and cybersecurity matters, including:

- Identifying state and federal privacy and data security laws that might apply to a particular business and developing policies and procedures to comply with these laws (i.e. employee privacy, financial privacy, healthcare privacy, marketing privacy)
- Implementing compliant document management and data retention plans
- Drafting and negotiating privacy and data security provisions in contracts (i.e. service provider contracts, vendor contracts and other types of agreements)
- Reviewing and addressing privacy and data security obligations and liabilities in vendor contracts supplied to clients by vendors to mitigate or reallocate risks
- Risk management and cyber insurance advise, including cybersecurity policy negotiation and procurement
- Post-breach investigation and response, including potential post-breach reporting and notification obligations, counseling and subsequent litigation
- Responding to Civil Investigations (CID's) undertaken by governmental authorities following the reporting of a data or cybersecurity breach or event
- Privacy-related claims and disputes.

Our Service Difference

We place a cultural emphasis on individualized attention to every representation, focusing on responsiveness, lean staffing, efficiency and results. When litigation is necessary, we often do it with fewer lawyers than our opponents while remaining more accessible to our clients when needed.

Our commercial litigation lawyers are also keenly aware of the business context in which litigation decisions must be made, and they make special efforts to understand the unique business and industry background of each client as it pertains to any assignment.

We understand and appreciate that a client is entrusting the value of their business to us when they turn to us as trial advocates, and we take that seriously. In fact, the very structure of our firm is client-focused, providing incentives to work collaboratively and share information in order to support our clients to the fullest while discouraging any attitudes or behaviors that interfere with the rendering of superior client service.

Representative Matters

Counseling and Other Services for a Company Entering into Content Development and Course-Load Distribution Agreements

Represented an online educational service provider, providing data privacy counseling and other services for a company entering into content development and course-load distribution agreements, including the establishment of a subsidiary in India.

Credit Card Privacy and Security Issues and Product Liability Matters

Provided advice and litigation services to a high-end electronics retailer regarding credit card privacy and security issues and product liability matters.

Inadvertent Release of Independent Contractor financial Information by a Third-Party Vendor

Represented an on-line educational service provider in connection with the inadvertent release of independent contractor financial information by a third-party vendor

Inadvertent Release of Protected Personal Information During the Course of Development and Construction Activities

Provide guidance and advice to nationally recognized furniture retainer in connection with data privacy matters resultant from the inadvertent release of protected personal information during the course of development and construction activities.

Outside U.S. General Corporate Counsel to a Leading Chinese Online Media, Communications, Search, Online Gaming, and Mobile Value-Added Services Company

Acted as outside U.S. general corporate counsel to Sohu.com, a leading Chinese online media, communications, search, online gaming, and mobile value-added services company (NASDAQ-traded) providing numerous services, including data privacy and risk management

Patented Software as a Service (SaaS) Company Providing Services to Major National Retailers

Represented a patented software as a service (SaaS) company providing services to major national retailers using proprietary algorithms in connection with all of its technology transactions in the areas of corporate, finance, contracts, retailer agreements, terms of use and privacy, data protection and use policies.

Potential Release of Personal Information on Account of Vendor Supplied POS Software

Represented Boston area restaurant group in connection with the investigation into and response to a potential release of personal information on account of vendor supplied POS software.

Drafting and Negotiating Privacy and Data Security Provisions in Contracts

Drafting and negotiating privacy and data security provisions in contracts (i.e. service provider contracts, vendor contracts and other types of agreements)

General Corporate Representation of Software Company

Representation of a developer of natural language and data asset management software, on matters including \$15M round of venture financing, software licensing, strategic acquisition and relationship matters, and general corporate representation.

Identifying State and Federal Privacy and Data Security Laws That Might Apply to a Particular Business

Identifying state and federal privacy and data security laws that might apply to a particular business and developing policies and procedures to comply with these laws (i.e. employee privacy, financial privacy, healthcare privacy, marketing privacy)

Implementing Compliant Document Management and Data Retention Plans

Massachusetts Attorney General Enforcement Action Based on a Data Privacy Breach

Represented Boston restaurant group in connection with a Massachusetts attorney general enforcement action based on a data privacy breach and the Commonwealth's data privacy law, G.L. c. 93H.

Post-Breach Investigation and Response

Post-breach investigation and response, including potential post-breach reporting and notification obligations, counseling and subsequent litigation

Privacy-Related Claims and Disputes

Responding to Civil Investigations Undertaken by Governmental Authorities

Responding to Civil Investigations (CID's) undertaken by governmental authorities following the reporting of a data or cybersecurity breach or event

Reviewing and Addressing Privacy and Data Security Obligations and Liabilities in Vendor Contracts

Reviewing and addressing privacy and data security obligations and liabilities in vendor contracts supplied to clients by vendors to mitigate or reallocate risks

Risk Management and Cyber Insurance Advise

Risk management and cyber insurance advise, including cybersecurity policy negotiation and procurement

Preparation of Commercial Agreements for a Publicly-Traded Technology Company

Prepared commercial agreements, including privacy and security matters, for the deployment of telemedicine networks by a publicly-traded technology company.

Prepare Privacy and Other Policies Regarding Digital Presence

Prepared privacy and other policies for digital presence of numerous national and international ventures.