Privacy & Data Security

Primary Contact

Eva Novick
Special Counsel
eva.novick@millernash.com
503.205.2472 | Portland Office

Sean D. O'Brien
Partner
sean.obrien@millernash.com
503.205.2360 | Portland Office

Brian Esler
Partner
brian.esler@millernash.com
206.777.7415 | Seattle Office

Companies collect, store, and process a wide range of personal information from customers and employees. Whether the data includes customer bank accounts, credit card information, or employee social security numbers, all businesses are custodians of sensitive data that are bound by privacy and security regulations.

Our attorneys advise clients on data security best practices, legal requirements, and industry-specific rules in an ever-changing landscape. In the event of a data breach, we work with companies to contain the breach, comply with notice requirements, and develop a strategic plan to prevent further issues.

Compliance

A patchwork of state and federal laws, and industry-specific rules, govern data security and the collection and use of data. We help our clients understand these regulations and draft information security policies to ensure compliance. We also help our clients make sure that they are providing proper notifications regarding how data is collected, stored, and used.

- We advise on a broad range of compliance issues, including:
- Washington's My Health My Data Act (MHMD)
- California Consumer Privacy Act (CCPA)
- General Data Protection Regulation (GDPR)
- Telephone Consumer Protection Act (TCPA)
- Family Educational Rights and Privacy Act (FERPA)
- Website privacy policies—including drafting, reviewing, and/or revising policies to accurately disclose how websites are collecting, storing, and using data.

Data Breach

Our attorneys have assisted local and international companies, large and small, that have experienced a data breach. We help companies understand their legal obligations, investigate the source of the breach, develop a strategy for an appropriate response, and notify regulators and/or affected individuals. Our attorneys work with in-house counsel and IT departments in various industries on breach response.

When a data breach results in litigation, regulatory investigations, or other disputes, our team is well positioned to provide strategic guidance and defense. Drawing on the firm's extensive litigation capabilities, we represent clients in cybersecurity-related disputes, including data breach class actions, consumer and employee claims, business-to-business disputes, and government and regulatory enforcement actions. By combining incident response and compliance counseling with experienced litigation support, we help clients navigate the full lifecycle of a data security event.

Data Security Audits

Every company should establish and regularly update its policies on secure receipt, storage, and transmission of consumer and employee data. We help companies examine their practices, identify the data they are collecting, storing, and transmitting, and understand what the law or other rules require them to do regarding that data. With that information in hand, we help clients develop policies that are both compliant and compatible with their business goals. Once these policies are implemented, we provide continual updates to reflect new requirements and best practices.

Vendor Contracts, Risk Transfer & Insurance

Our attorneys understand the intersection of contractual law, insurance law, and data security. We have reviewed and negotiated hundreds of vendor contracts that involve these issues, including cloud computing, information technology, networking, data center, and database agreements in domestic and international transactions. We have extensive experience working with in-house legal departments, engineers, sales teams, and related departments.

Employee Training & Presentations

Keeping data secure and ensuring that data policies are properly executed requires awareness and understanding from all employees who handle that data. Our attorneys regularly give presentations and provide in-house training on the data security laws that pertain to a company and the best practices to avoid unauthorized persons from gaining access to data.

Representative Experience

We advise on a broad range of compliance issues, including:

- Assisted major global diversified manufacturing and marketing company with a data breach of social security numbers and other sensitive employee data.
- Assisted nonprofit with an identity theft hacker intrusion on its human resources database. We drafted a data breach response process and developed a press release.
- Assisted fast-food franchise managing a data breach caused by an IT software vendor. In conducting maintenance on their system, the vendor inadvertently took down the system's security.
- Advised clinic in responding to a breach of patient health information. We also advised on issues regulated under the Health Insurance Portability and Accountability Act (HIPAA).
- Advised global internet company with developing and implementing responses to the Edward Snowden revelations regarding monitoring of internet traffic.
- Advised government entity with homeland security issues regarding a data breach response program and information security issues. We trained in-house legal and IT staff on data security issues and participated in a simulated data breach exercise.

Data Security Audits

- Data Security audit for an educational institution that resulted in identifying different procedures for data handling among various departments. In addition, the audit revealed an outdated FTC Red Flag policy, which we helped resolve.
- Assisted with an audit on behalf of a public entity that was preparing to collect credit card payments. Our attorneys helped the agency develop its strategy for complying with the Payment Card Industry Data Security Standard (PCI DSS).
- Assisting various clients with developing and improving incident response plans.
- Assisting legal and IT staff for a government transportation entity regarding data security.
- Assisting a regional bank on compliance with Federal Financial Institutions Examination Council (FFIEC) data security standards and preparing for a regulatory audit.
- Assisting companies with in-house training on best practices for preventing unauthorized access to data.

Vendor Contracts, Agreements, & Insurance

- Regularly advising one of the largest global internet companies on domestic and international data security issues arising in transactions involving internet networking, data centers, and related vendor contracts.
- Negotiated hundreds of contracts and agreements that involved sensitive data security and privacy issues, including cloud storage, sharing sensitive information, data centers, networking, colocation, dark fiber, IP transit, communications services and equipment, complex server systems, wireless networks, equipment leases, device trials, spectrum leases, cell tower leases, and many other issues. These transactions were for services in 35 different countries in North America, South America, Africa, Europe, and Asia.
- Advised companies in multiple industry sectors—including banks, construction firms, educational institutions, and manufacturing and retail—on cyber-insurance and other risk transfer strategies in vendor and other contracts.