HUSCH BLACKWELL

DATA PRIVACY & CYBERSECURITY

Husch Blackwell's Data Privacy & Cybersecurity law team helps organizations leverage the value of their information assets while satisfying compliance requirements and controlling risk. Our data privacy lawyers possess insights and solutions enabling clients to achieve firmer control over their information while making meaningful progress toward long-term data security objectives.

Our team of data privacy & cybersecurity attorneys regularly counsel clients on complying with existing and emerging data privacy and information security laws, including the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act of 2018 (CCPA), the Colorado Privacy Act of 2023 (CPA), and state information security statutes. Clients also rely on our Byte Back blog for legal trends in data privacy and cybersecurity.

Our law firm helps safeguard clients against cybertheft and other unauthorized disclosures of protected information. We assess cybersecurity risks and provide best practices guidance for preparing for data security incidents. When data breaches are suspected, our team of Breach Response lawyers responds immediately to minimize damage to business operations and reputation.

Privacy

Our team of data privacy lawyers advises on compliance with HIPAA, the Gramm-Leach-Bliley Act, FERPA, TCPA, the CAN-SPAM Act, EFTA, FCRA/FACTA,

"The firm has substantial trial experience, which is essential to be effective in litigation, and has the confidence to take matters to trial."

— Chambers USA 2019 —

Contact Information

Erik Dullea
303.749.7270
erik.dullea@huschblackwell.com

Mindi S. Giftos
608.234.6076
mindi.giftos@huschblackwell.com

David M. Stauss
303.892.4429
david.stauss@huschblackwell.com

COPPA and state privacy laws. We evaluate and develop information security compliance plans, conduct compliance training, and prepare and negotiate information privacy-compliant agreements. We also defend clients against litigation and regulatory investigations. We respond to Office for Civil Rights enforcement actions, often negotiating dismissals; litigation, including class actions; and Telephone Consumer Protection Act (TCPA) enforcement proceedings.

We are uniquely situated to advise colleges and universities on Education Privacy Law matters, including FERPA guidance.

Cybersecurity

The best time to assess risk, secure data and plan for a breach is before a cybersecurity incident occurs. Husch Blackwell helps clients guard against cybertheft, cyberextortion and other unauthorized disclosures of protected information. We assess cybersecurity risks and gaps, develop compliant and effective security controls, educate employees, assess cyberliability insurance coverage and establish defensible records retention plans.

Breach response

When protected information is compromised or lost, our Breach Response attorneys move immediately to determine legal responsibilities and next steps in an effort to minimize damage. Our team has identified 10 channels of activity, from notification to insurance coverage, that must occur after a data breach. We guide clients in laying groundwork that will ensure these

activities are handled with minimal confusion, cost, risk and delay during a rapidly unfolding, high-stakes breach crisis.

Representative Experience

Developed records retention schedules, file plans, and information management policies for an $83 billion asset management and financial planning firm, and for a financial services and national bank holding company with $33 billion in managed assets.

Represented clients in health information data breaches involving thousands of patients' medical records. Advised clients on appropriate responses and best practices to protect patient data.

Developed legal hold processes for organizations in the energy, retail, and manufacturing industries.

Developed and validated records retention schedules for multistate power and gas utilities and pipelines.

Provided information management training to over 900 corporate personnel at a professional services company.

Drafted medical staff bylaws, rules, and regulations, including HIPAA-compliant policies and procedures.

Developed records retention schedules and advised on records retention and information management policies, procedures, and implementation for a Fortune 100 pharmacy benefits management company.

Advised regarding legacy data remediation for a regulated

public utility.

Performed HIPAA Security Rule risk assessments for covered entities and business associates, including Long Term Care facilities and Third Party Administrators.

Validated records retention schedules for hospitals and health systems, pharmaceutical and biotechnology companies, pharmacy benefit management companies, and medical equipment manufacturers.

Delivered processes and presented training on compliant records management and disposal for organizations undergoing corporate headquarters moves in the professional services, retail and manufacturing industries.

Represented clients in health information data breaches involving thousands of patients' medical records. Advised clients on appropriate responses and best practices to protect patient data.

Represented a specialty physician group practice whose computer system was compromised by the download of patient records. Our representation led to the return of patient records and ensured compliance with HIPAA and HITECH. Our client recouped all costs relating to this matter.

Counseled large pharmaceutical client that manages a significant amount of protected health information in analyzing its de-identification practices to ensure compliance with HIPAA while continuing its practice of transmitting de-identified information to third parties

without individual authorization. We partnered with statistical consultants to develop a unique approach to utilize the protected health information while maintaining compliance with HIPAA. We also worked with our client to develop sophisticated guidelines to help them make use of the de-identified information.

Defended numerous healthcare clients in HIPAA investigations, including breaches involving 500 or more individuals. Additionally, the attorney provided essential testimony in court cases regarding privacy and security requirements under state and federal law.

Provided a complete analysis of privacy law implications associated with the comingling of data from global consulting SaaS company's various clients to monetize that value. Specifically analyzed the impact of the California Consumer Privacy Act, California Privacy Rights Act, Colorado Privacy Act and Virginia Consumer Data Protection Act on the clients' various proposals, as well as the impact of Canadian federal privacy laws.

Performed extensive review and revision of online privacy policies and terms of use in relation to numerous websites and apps for one of the top mortgage lenders in the United States. Also provided counsel on how to implement new terms of use to ensure proper enforceability as well as advice and counsel on avoiding session replay technology lawsuits. Also advised on Gramm-Leach-Bliley Act, California Consumer Privacy Act and California Privacy Rights Act compliance.

Represented global private equity firm in numerous privacy projects involving the investment of millions of dollars in tech start-ups. Representation included conducting extensive privacy compliance due diligence and negotiating contractual representations and warranties.

Advised client on privacy law compliance issues arising out of its deployment of new tablet-based software in the United States, Canada, Europe and Asia. Work included counselling on product design, including data minimization and drafting a privacy policy.

Assisted university foundation with numerous privacy law compliance issues, including drafting its new data processing agreement with the university, assisting with FERPA compliance questions, responding to a data security incident, and conducting vendor due diligence.

Counseled client pivoting from online business-to-business company to business-to-consumer company. Work included revising privacy policy, terms of use and terms of service, as well as providing advertising compliance advice in relation to marketing efforts, including CAN-SPAM compliance, and avoiding sessions replay technology lawsuits.

Served as breach counsel and handled all aspects of phishing attack experienced by large state university.

Served as breach counsel for state university foundation when it was part of a data breach suffered by a third-party provider. Worked with the Chief Information Security Officer to analyze the regulatory framework governing the

matter and coordinate the foundation's response.