McDermott
Will & Emery

Global Privacy & Cybersecurity

OVERVIEW

McDermott's world-class Global Privacy and Cybersecurity team includes more than 50 privacy and cybersecurity lawyers advising clients on the statutory, regulatory and enforcement regimes that govern the collection, use and disclosure of data in the United States, Europe, Asia and elsewhere.

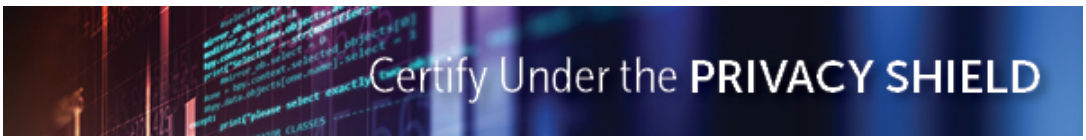
We have extensive experience advising on the full range of data privacy and protection laws, industry standards and issues. Our lawyers regularly counsel clients on US and international data-use issues, data transfers, and privacy compliance under US and foreign laws. We conduct in-depth privacy/cybersecurity risk assessments, often in the context of mergers, acquisitions and other domestic and cross-border transactions.

In the event of data breaches or alleged improper use of data, we provide swift, effective cybersecurity incident response and represent clients in litigation and government investigations. Our practice includes lawyers with deep experience in health care data privacy and related litigation. Among recent examples of our trial and appellate work, we obtained a victory before the US Supreme Court in one of the most important recent privacy cases, *Gobeille v. Liberty Mutual*, in which the court held that self-funded insurance plans are exempt from a Vermont law purporting to compel disclosure of health information to the state.

Several of our privacy lawyers have won awards or recognitions in the privacy field, including honors from *The National Law Journal*, *The Legal 500 UK*, *Chambers USA* and other leading journals and legal ratings agencies.

Our team's experience includes:

- Handling hundreds of cyber incidents, including massive data breaches involving all 50 US states and over 100 countries
- Representing clients in privacy and cybersecurity litigation and government investigations regarding the collection, use or exposure of consumer, patient and other information
- Coordinating with EU, US and other national regulators on cyber incidents
- Developing data privacy management programs
- Advising executives and boards of directors on cyber-risk priorities and facilitating breach tabletop exercises for key leadership
- Conducting privacy due diligence in M&A transactions and structuring deal terms to mitigate risk
- Establishing and upgrading incident-response policies
- Creating vendor risk protocols and contract provisions
- Assessing privacy/cybersecurity risks facing employee benefit plans
- Evaluating the EU/US Privacy Shield and other data-transfer alternatives and implementation strategies
- Advising on compliance with the EU's General Data Protection Regulation (GDPR)



KEY CONTACTS

Mark E. Schreiber
Partner

Michael G. Morgan
Partner

Daniel F. Gottlieb
Partner

RESULTS

- Advised an international chemicals and specialty materials producer regarding the global implementation of a General Data Protection Regulation (GDPR) compliance program, including the assessment of current practices, the review and amendment of policies, processes and documentation, and the appointment of a central data protection officer (DPO)
- Handled a series of large data breaches involving personnel records of employees in the United States and around the world and advised our client on its obligations under the laws of every US state and more than 50 countries; managed communications with the affected employees and various government regulators; and persuaded regulators to forego any claim against our client
- Obtained a victory before the US Supreme Court in one of the most important recent privacy cases, *Gobeille v. Liberty Mutual*, persuading the Court to hold that self-funded insurance plans are exempt from a Vermont law purporting to compel disclosure of health information to the state
- Created a GDPR-compliant privacy program for a US retail products manufacturer covering the legal grounds of data processing, external privacy notices, internal privacy guidelines, international data transfers and online data collection
- Advised a global medical device company on certification of compliance with the US-EU Privacy Shield, including data mapping, review and evaluation of internal and external policies and procedures, and amendments to vendor contracts

- Advised a multinational hotelier in creating data analytics strategies, external marketing strategies and revising online privacy policies to disclose such strategies
- Advised a US manufacturer of industrial products on the privacy implications of selling and remotely operating smart devices in the EU
- Advised a US health care provider on the legal prerequisites of using European patient data for scientific purposes
- Advised an international university regarding GDPR compliance, including the scope of application of the GDPR to activities in the EU, the lawful grounds for processing personal data (such as consent), appointment of a DPO, and various other GDPR compliance issues
- Developed online privacy policies and terms of use for clients in a range of industries, including aerospace, alternative energy, luxury fashion, electronic medical records (EMR) management, mobile apps, technology, small business consulting, and health care and managed care plan services
- Advised a vertically integrated health care provider and payer regarding all aspects of the acquisition, implementation and deployment of an enterprise data warehouse (EDW), including negotiating software and hardware acquisition and implementation services agreements, analyzing HIPAA and other regulatory and data stewardship requirements for combining provider and payer data into an integrated EDW, and assessing implications for achieving meaningful use under the Medicare Electronic Health Records (EHR) Incentive Program
- Advised dozens of clients on standard contractual clauses and similar agreements for transferring personal data from the EU to jurisdictions without EU-level privacy protection standards
- Advised clients regarding DPO locales and obligations, breach-reporting preparation (*e.g.*, localizing EU forensics, call centers and breach response vendors), cyber risk and data protection insurance, and data collection, storage, use and related risk assessments under GDPR
- Created and designed a corporate privacy and cybersecurity program for a major multinational company, including work tasks, team designations, high-medium-low priority designations, and a presentation to senior leadership team on privacy and cybersecurity risks
- Handled the response to a series of incidents involving the compromise of patient information at a leading California hospital, including overseeing the forensic investigation into the incidents, advising on the applicable legal obligations (*e.g.*, under HIPAA and state laws), preparing a notification and communication program, and recommending appropriate mitigation measures
- Advised a global utility and internet-of-things solution provider on obligations under data protection laws of Canada and Hong Kong
- Represented a major e-commerce company in a dispute with its technology provider relating to the adequacy of the security in the provider's solution, including the encryption algorithm used to secure the transactions between the e-commerce company and its customers
- Advised an electronic health records (EHR) vendor regarding the creation and deployment of de-identified health data sets from patient information received from provider customers, including review and negotiation of a HIPAA de-identification opinion, development of data privacy and security policies and procedures, and

drafting and negotiation of agreements with pharmaceutical and biotech companies seeking access to the de-identified data set

- Assisted a large emergency medical physician practice with all aspects of its response to a theft of a portable hard drive containing medical billing information for more than 175,000 patients from over 50 jurisdictions, including drafting the template breach notification letter, breach reports to the Office for Civil Rights (OCR) and state regulators, talking points for call center operators, press releases and media notices, and an indemnification claim to the medical billing agency; after responding to OCR's investigative data requests, the matter was successfully resolved with OCR without penalty; in conjunction with counsel to the billing agency, we obtained the dismissal, at the motion to dismiss stage, of a related consumer class action
- Created a vendor-management program to deal with a multinational client's compliance obligations in selecting vendors capable of protecting consumer personal information, including a due diligence checklist, template privacy and security provisions, and negotiating tips
- Advised a health IT vendor on the development, deployment and operation of an mHealth app, including negotiating developer agreements, alpha/beta agreements and related commercial agreements, advising on privacy and security requirements for mobile and connected devices, counseling on consumer data stewardship, and drafting privacy policies and other consumer-facing documents
- Advised an international human resources services provider on revising its suite of online privacy policies to ensure compliance with EU and US law and preparing for foreseeable future developments of the pertinent law
- Advised a global fitness products company with the rollout of mobile and connected health and fitness functionality
- Advised an electronic health record (EHR) vendor on all aspects of launching a telemedicine app, including development of the app's terms of use, privacy policy and patient informed consent
- Advised a national telemedicine company on the development of an integrated and coordinated virtual care and in-person primary care model and related data-sharing tools
- Advised an informatics company on the development of a research data acquisition and analysis platform that included federally and privately sourced data
- Advised a national multi-hospital consortium on its regulatory compliance and contract strategy for the development, implementation, maintenance, ownership and licensing of a comparative database and decision support system that involved electronic information exchange, aggregation and analysis by and among its more than 200 member hospitals