

PRIVACY & DATA SECURITY



OVERVIEW

Modern businesses have an ever-greater need to collect, store, transmit, and use sensitive data, including credit card information, patients' protected health information (PHI), personally identifiable information (PII), and proprietary business information. With increased use and storage of data comes increased risk of cyberattack or breach. It is not a question of if—but when—a business will be targeted and become the victim of a cyberattack or experience a data breach. Businesses must be prepared to respond immediately in the event of an incident.

These cybersecurity risks are not limited to large corporations or high-tech firms. Even small or medium traditional “brick and mortar” businesses use point of sale, accounting, content management, and other systems that contain critical and sensitive data—either in-house or through cloud-based systems hosted by vendors and contractors.

As the risks have increased, state and federal governments have implemented increasingly complex and stringent information security laws and regulations for the privacy and security of customer, patient, and employee information. At the same time, consumers have demanded greater data protection, transparency, and accountability from companies with whom they do business. Preparing for and responding to these data protection challenges are vital for any business to survive and prosper.

Foulston's attorneys use their broad risk management experience to help clients understand, prepare for, and respond to every segment of the information life cycle. Whether you are acquiring a software system, engaging a data-hosting provider, outsourcing data-intensive functions to a vendor, drafting privacy and data security policies and procedures, auditing your data protection practices, engaging in the sale or licensing of data, responding to a data breach or cyberattack, or defending a class-action or other data litigation, Foulston's attorneys have the background and experience to advise, counsel, represent, and defend clients in all aspects of the data-privacy and cybersecurity spectrum.

AREAS OF REPRESENTATION

Data Security Compliance, Counseling, and Risk Management

We counsel clients on network security and data security practices and risk management methods, including risk identification and assessment, risk mitigation, development of procedures and protocols to help prevent and deter cybersecurity breaches, and insurance coverage analysis. Our experience includes:

- Using National Institute of Standards and Technology (NIST) standards to assess company privacy, security, and data protection and information security management policies and procedures based on our extensive experience in regulated industries.
- Preparing employment agreements and policies, including Bring Your Own Device (BYOD) policies and other issues related to employee-supplied smartphones and tablets.
- Advising clients on employment issues regarding employee data privacy, including nondisclosure of confidential and proprietary information and competitive intelligence and trade secrets.
- Preparing Health Insurance Portability and Accountability Act (HIPAA) privacy, security, and breach notification policies and procedures, including the use of mobile and medical devices.
- Working with clients and security experts to prepare policies and modify business forms to incorporate data security principles in client agreements and third-party service provider contracts.
- Analyzing coverage and counseling clients concerning insurance policies for cybersecurity issues.

Privacy and Security Regulation

We leverage our extensive experience in the financial services, healthcare, information technology, trade, and other regulated industries to assist clients in complying with state, federal, and international information privacy and security requirements. Our experience includes:

- Advising clients on data privacy and security laws and regulations in regulated industries and practices, including the Gramm-Leach-Bliley Act, USA Patriot Act, HIPAA, the Children's Online Privacy Protection Act, the Federal Trade Commission's (FTC) Identity Theft Red Flag Rules, and other federal and state laws.
- Preparing business associate agreements, business partner agreements, and other contractual provisions to pass through data privacy and security requirements.
- Assisting and counseling clients on policies and procedures to satisfy the United States Department of Commerce's Safe Harbor framework for compliance with the European Commission's Directive on Data Protection and the Swiss Federal Act on Data Protection, including self-certification.
- Drafting and reviewing website data privacy and security policies to comply with applicable federal and state requirements, including the enforcement actions and guidance under the FTC's Act.

Transactions Involving Data

Our merger and acquisition, commercial transactions, information technology, and intellectual property attorneys bring their breadth of experience to bear on transactions that include the transfer or licensing of proprietary and protected information. Our experience includes:

- Assisting and counseling with data privacy and security due diligence investigations.
- Preparing and negotiating pre-transaction documents and sale and licensing agreements.
- Structuring joint venture and acquisition entity arrangements to comply with applicable data and export control restrictions.
- Evaluating and negotiating security consulting and securing technology licensing agreements.

Data Breach Response

We assist our clients in their preparation for potential data breaches to help minimize their potential legal exposure. Together with technical experts and consultants, we investigate incidents to determine the scope of a breach, analyze what is required under applicable laws, and counsel clients concerning compliance with legal requirements and best practices. We assist our clients with:

- Drafting policies and procedures and contractual provisions regarding discovery, investigation, remediation, and reporting of breaches.
- Advising clients concerning the legal aspects of data security breach incidents, including protection of the breach investigation under attorney-client privilege to the greatest extent possible.
- Determining legal obligations for data breach response and notification and disclosure obligations under the federal and state regulations, including compliance with state security breach notification statutes and other state requirements, breach notification requirements of the Gramm-Leach-Bliley Act, and the HIPAA Breach Notification Rule.
- Assisting clients in presenting claims under cyber insurance policies.

Data Breach and Cyberattack Litigation and Counseling

Our litigation attorneys bring suits against those who commit cyberattacks and steal or misappropriate our clients' proprietary and protected information. Our attorneys are also experienced in defending our clients against governmental investigations and actions resulting from breaches of their data. Our experience includes:

- Litigating cases involving intellectual property infringement and information and data misappropriation suits, including obtaining preliminary and permanent injunctions.
- Enforcing cyber insurance policies.
- Representing clients with collateral litigation resulting from breaches of personally identifiable information and other protected information.
- Defending government investigations and enforcement actions and successfully negotiating resolutions with regulators, including actions involving the Office for Civil Rights (OCR).

Export Control, National Security, and Law Enforcement Investigations

- Preparing policies and practices for and advising clients concerning export control compliance, including ITAR, EAR, and OFAC.
- Counseling clients who have received Kansas or federal law enforcement and governmental requests for access to information.
- Defending executives and corporations in white collar investigations relating to compliance issues.

RELATED LINKS

- US Computer Emergency Readiness Team
- Kansas Office of Information Technology Services
- FBI—Cyber Crime
- FTC Act Section 5 Examination of Unfair/Deceptive Practices
- Electronic Communications Privacy Act
- Prosecuting Computer Crimes – Justice Dept.
- Federal Trade Commission – Privacy and Security

ISSUE ALERTS

2020

- Coronavirus: Maintaining Privacy and Data Security with a Remote Workforce

PUBLICATIONS

- Kansas Sectorial Privacy Overview
- OneTrust DataGuidance (April 2022)
- Lex Mundi Global Data Privacy Guide
- Kansas Section (2022 ed.)

ATTORNEYS/OTHER PROFESSIONALS

PRIMARY CONTACTS



DANIEL J. BULLER

Partner

T: 913.253.2179
dbuller@foulston.com

ADDITIONAL SUPPORTING MEMBERS



BROOKE BENNETT AZIERE

Partner

T: 316.291.9768
baziere@foulston.com



JEFF P. DEGRAFFENREID

Partner

FOULSTON

ATTORNEYS AT LAW

T: 316.291.9788
jdegraffenreid@foulston.com



HOLLY A. DYER

Partner

T: 316.291.9773
hdyer@foulston.com



WILLIAM P. MATTHEWS

Partner

T: 316.291.9556
bmatthews@foulston.com



SARAH C. OTTO

Partner

T: 913.253.2195
sotto@foulston.com



FOULSTON

ATTORNEYS AT LAW

TERESA L. SHULDA

Partner

T: 316.291.9791
tshulda@foulston.com



CHARLES R. HAY

Senior Partner

T: 785.354.9413
dhay@foulston.com



GORDON G. KIRSTEN II

Special Counsel

T: 316.291.9538
gkirsten@foulston.com