



Privacy, Data Security, and AI

Overview

Our Privacy, Data Security, and AI Group understands that the effective protection and management of information is critical for an organization to operate successfully. Businesses must comply with an increasingly complex web of state, federal, and international laws and regulations, including comprehensive state privacy statutes (e.g., the CCPA/CPRA and analogous laws), sector-specific federal requirements, and cross-border transfer frameworks, all designed to protect commercially sensitive data and personally identifiable information. Our inter-disciplinary group of attorneys provides clients with practical solutions to comply with the requirements governing the gathering, storage, transfer, and use of information.

Our attorneys counsel clients regarding legal and practical techniques intended to maximize protection and minimize or avoid risks that may compromise sensitive and proprietary business information. In the event of a breach, we work closely with clients and internal and external response teams, including forensic investigators and accountants, computer consultants, press and media advisors, and other crisis management providers, to efficiently and effectively address the company's immediate and long-term needs, including contractual notification obligations to vendors, customers, and business partners.

Our trial attorneys have the courtroom experience needed to address our clients' privacy and data security litigation needs. We also provide the skills and experience in dealing with obligations of immediate disclosure, response, and remedial measures in the face of a data privacy or security breach.

For a description of our HIPAA and Medical Privacy Practice, click [here](#).

ARTIFICIAL INTELLIGENCE AND EMERGING TECHNOLOGY

Data privacy and security questions arise in virtually every AI deployment. We advise clients on the obligations that accompany AI use, including compliance with evolving state, federal, and international privacy frameworks as they expand to address AI-specific risks such as automated decision-making, personal data used in model training, and the collection and processing of sensitive information by AI-driven systems.

We also help organizations develop and implement AI governance frameworks, acceptable-use policies, and vendor due diligence protocols, including negotiation of data processing agreements, security exhibits, and contractual safeguards allocating liability for AI-related data incidents, all of which address the unique data privacy and security risks AI systems

present, from biometric data processing and algorithmic decision-making to regulatory reporting obligations and third-party data-sharing. When an AI-related incident occurs, whether involving unauthorized data exposure, improper data collection, or regulatory inquiry, our team draws on the same breach-response and investigation capabilities that define our broader practice to help clients act quickly, meet disclosure obligations, and manage reputational risk.

Our trial attorneys are prepared to handle AI-related privacy and data security disputes and enforcement actions, including class action claims arising from biometric or personal data used in AI systems, government investigations into AI-related data privacy or security failures, and regulatory proceedings involving AI-driven data processing practices.

AREAS OF EMPHASIS

Tucker Ellis assists clients of all sizes across industries in data privacy incidents that implicate:

- Business Litigation (individual and class action litigation)
- Financial Services Counseling (Gramm-Leach-Bliley Act/Sarbanes-Oxley)
- General Data Protection Regulation (GDPR)
- Data Processing Agreements and Vendor Security Assessments
- HIPAA/HITECH Enforcement and State Medical Privacy Laws
- OCR Audit Preparation
- Insurance Coverage
- Information Technology (storage, use, and access to personal and confidential information, both internal and external)
- Risk Avoidance (technological and legal initiatives)
- Regulatory Compliance Reporting
- Employment Counseling
- Biometric Data Analysis
- State and Federal Cybersecurity Laws
- State Comprehensive Privacy Laws
- PCI-DSS
- Trade Secrets
- White Collar Criminal Defense
- Internal Corporate Investigations and Counseling

PRESENTATIONS

- “Data Privacy in Education Tech,” International Association of Privacy Professionals (April 2021)

- “Bracing for the New Normal in Data Privacy: GDPR, CCPA, and Other Initiatives Impacting the Business World in 2020 and Beyond,” 2019 In-House Counsel Summit, Tucker Ellis LLP, Cleveland, Ohio (November 2019) “
- “Preservation, Discovery, and Presentation of Cyber Evidence,” IADC Webinar (June 2019)
- “GDPR and International Compliance” and “Health Care Sector Deep Dive,” Cybersecurity & Privacy Protection Conference 2019, Cleveland, Ohio (May 2019)
- “Global Security Risk Management Update: Impact on Cyber, Intellectual Property, Personal and Corporate Physical Security,” Cleveland Metropolitan Bar Association, Cleveland, Ohio (May 2019)
- “The Impact of GDPR on Enforcing Intellectual Property Rights on the Internet,” Harvard Law School, Cambridge, Massachusetts (March 2019)
- “Avoiding Legal Liability,” The Information Security Summit, Cleveland, Ohio (October 2018)
- “Workplace Privacy: Developments in Monitoring and Use of Genetic Information,” Ohio State Bar Association WebCast (September 2018)
- “Cyber Ohio Business Summit on Cyber Risk Assessment,” Office of Ohio Attorney General Mike DeWine, Columbus, Ohio (March 2018)
- “Technology in the Workplace: Data Protection in Practice,” Warren Regional CLE, Ohio State Bar Association, Warren, Ohio (May 2017)
- “Regulating Information: A Candid Conversation About HIPAA and Privacy,” Cleveland-Marshall College of Law, Cleveland, Ohio (April 2017)
- “Healthcare Cybersecurity and Privacy Litigation,” Health Care Law Update & Medical/Legal Summit 2017, Cleveland Metropolitan Bar Association/Academy of Medicine Education Foundation/The Academy of Medicine of Cleveland & Northern Ohio, Cleveland, Ohio (March 2017)
- “HIPAA Best Practices and Audit Readiness,” Health Action Council Webinar (February 2017)
- “Understanding & Navigating Cyber Liability Policies,” Advanced Issues in Insurance Coverage Law, Akron Bar Association, Akron, Ohio (December 2016)
- “Healthcare Update – Regulations, HIPAA, and Risk Avoidance,” 2016 In-House Counsel Summit, Tucker Ellis LLP, Cleveland, Ohio (October 2016)
- “Cyber Security Month – Security Panel,” Case Western Reserve University, Cleveland, Ohio (October 2016)
- “A Practical Guide to Your Incidence Response Plan,” Practical Tips and Tools to Deal with Cybersecurity Challenges, Tucker Ellis LLP, Cleveland, Ohio (July 2016)
- “Identifying, Calculating, and Mitigating Covered Loss under New Cyber Liability Policies,” Cleveland Metropolitan Bar Association Insurance Law Section, Cleveland, Ohio (November 2015)

- “Surviving the Breach: Immediate Steps and Responses,” and “What Are the Risks: An Introduction to Exposures, Costs, and Trends,” Tucker Ellis Privacy and Data Security Risks: Are You Prepared?, Cleveland, Ohio (July 2015)
- “Protecting the Net: Cybersecurity,” Tucker Ellis/McGladrey Marching Through the Madness: Making Your Financial Services Team a Winner in Risk and Compliance, Cleveland, Ohio (March 2015)
- “Data Security: Managing the Crisis,” 2014 In-House Counsel Summit, Tucker Ellis LLP, Cleveland, Ohio (October 2014)
- “HIPAA HITECH Compliance Seminar: What Organizations and Their Business Associates Need to Know,” sponsored by Tri-C and JurlInnov (July 2013)
- “Technology and Cyber Risks – Exposures and Coverage Options,” Public Agency Risk Managers Association (May 2012)
- Webinar: “Great Ideas for Media and Technology in Schools.” Available online at <http://training.sia-jpa.org/Academy/ViewCourse.aspx?CourseID=24>
- Speaker at seminars on “Data Breach: Understanding the Risk and Managing a Crisis”
- Presented “Data Security Risks and Crisis Management” to individual firm clients
- “Navigating the Stringent Legal e-Discovery Requirements and Patient Confidentiality Concerns Associated with Electronic Documentation,” Advanced Forum on Healthcare Provider Disputes & Litigation, American Conference Institute, Chicago, Illinois (July 2012)
- “The Risks and Rewards of EMR: Meaningful Use or Tool for Abuse?,” 7th Annual National Medical Liability Insurance ExecuSummit, Mohegan Sun, Connecticut (September 2011)

PUBLICATIONS

- “The AI Vendor Contract Is Becoming More Important Than the Privacy Policy,” Tucker Ellis Client Alert (August 2026)
- “EU-U.S. Data Privacy Framework and New U.K. U.S. Data Bridge: Mechanisms to Support Growth for U.S. Businesses,” Tucker Ellis Client Alert (October 2023)
- “SEC Adopts Final Cybersecurity Disclosure Rules,” Tucker Ellis Client Alert (August 2023)
- “Federal Judge Vacates \$228M Damages Award in BIPA Trial and Orders New Damages Trial,” Tucker Ellis Client Alert (July 2023)
- “Illinois Supreme Court Holds BIPA Claims Accrue with Each Alleged Scan,” Tucker Ellis Client Alert (February 2023)
- “Illinois Supreme Court Holds Five-Year Statute of Limitations Applies to All BIPA Claims,” Tucker Ellis Client Alert (February 2023)
- “Are You Affected by the Blackbaud Ransomware Attack?,” Tucker Ellis Client Alert (August 2020)
- “Best Practices for Data Privacy and Cybersecurity in a Virtual Construction Work Environment,” *Construction Industry Executive* (May 2020)

- “Secure Your Home Workspace During the COVID-19 Pandemic,” Tucker Ellis Client Alert (March 2020)
- “Are You Ready for the California Consumer Privacy Act?”, Tucker Ellis Client Alert (July 2019)
- “Ohio Joins Growing Trend Requiring Cybersecurity Standards and Reporting Obligations for Insurance Industry,” Tucker Ellis Client Alert (February 2019)
- “Illinois Supreme Court Rules in Favor of Consumers in Landmark Biometric Data Case,” Tucker Ellis Client Alert (January 2019)
- “The Future Is in the Palm of Your Hand and in the Details of Your Eyes, Face, and Fingerprints as Businesses Handling Biometric Data Face a New Wave of Class-Action Litigation,” DRI’s The Business Suit (Vol. 22, Issue 4)
- “Cybersecurity Safe Harbor Against Data Breach Lawsuits Becomes Ohio Law,” Tucker Ellis Client Alert (August 2018)
- “California Passes Landmark Law Creating Broad Data Privacy Rights for California Residents,” Tucker Ellis Client Alert (July 2018)
- “GDPR Update: Your Questions About GDPR – Answered,” Tucker Ellis Client Alert (July 2018)
- “‘Injury in Fact’ Standing After Cambridge Analytica,” Law360 (June 2018)
- “GDPR Focus: How the European Union’s New Cybersecurity Measure Will Impact Your American Manufacturing Business,” Manufacturing Today (May 2018) “Assessing the Fine (Finger) Print: Biometric Data Is the New Frontier in Data Security and the Next Wave of Litigation,” Cleveland Metropolitan Bar Journal (May 2018)
- “Roundtable: Cyber Risk & Security,” Financier Worldwide (May 2018)
- “The SEC’s Latest on Disclosures: New Guidance Mandates Greater Attention to Cybersecurity Planning,” Corporate Compliance Insights (April 2018)
- “Countdown to the GDPR,” Manufacturing Business Technology (March 2018)
- “Countdown to the GDPR: What You Need to Know About the Impact of the European Union’s New Cybersecurity Measures on Your American Business,” Tucker Ellis White Paper (March 2018)
- “Proposed Legislation Seeks to Safeguard Ohio’s Election System Against Cyberattacks,” Tucker Ellis Client Alert (February 2018)
- “Lessons for Data Breach Lawyers from Product Liability,” Law360 (January 2018)
- “Ohio Bill Proposes Safe Harbor Against Breach Suits to Businesses Maintaining Recognized Cybersecurity Programs,” Tucker Ellis Client Alert (December 2017)
- “Data Security Breaches Land General Counsel on Chopping Block; Lessons from Yahoo!,” Tucker Ellis Client Alert (March 2017)
- “Don’t Let a Data Breach Derail the Deal,” Crain’s Cleveland Business (January 2017)
- “Enhancing Board Oversight of Cyber Risk – The Board’s Increasingly Important Role,” Corporate Compliance Insights (December 2016)

- White Paper and associated Proposed Internal Policies and Guidelines regarding proper use, access, and protection of technology, Internet, personal digital assistants (PDAs), and cellular telephones, and individual Technology User Agreements
- “Think Fast: The Potential for Tension Between Insureds and Data Security Insurers,” Bloomberg BNA’s Privacy and Security Law Report (August 2016)
- “The Greatest Cybersecurity Risk Comes From Within,” Law360 (September 2015)
- “Data Security Plans: Why Financial Institutions Must Continuously Assess and Update Their Data Security Plans,” Bloomberg BNA’s Corporate Law & Accountability Report (June 2015)
- “The ‘Heartbleed’ Bug and Responding to a Data Security Breach,” Tucker Ellis Client Alert (April 2014)
- “Data Security: What You Don’t Protect Can Cost You,” published in FOCUS, quarterly newsletter of the Association of Corporate Counsel Northeast Ohio Chapter (1Q2013)

MEDIA QUOTES

- “Why You Should Create a Forward-Thinking Privacy Policy,” InformationWeek (August 2019)
- “Banks Feeling the Heat Over Fintech Partners’ Cyber Risks,” Law360 (June 2019)
- “DC Circ. Piles Onto Standing Split With Data Breach Ruling,” Law360 (June 2019)
- “Data Breach Legislation Proposes Jail Time for CIO, HR Execs,” TechTarget (April 2019)
- “CCPA Compliance Begins with Data Inventory Assessment,” TechTarget (December 2018)
- “Legal Tech’s Predictions for 2019 in Cybersecurity and Privacy,” Legaltech News (December 2018)
- “Lawyers Weigh In on the Loews Hotel Biometric Data Misuse Case,” Hospitality Technology (October 2018)
- “The Coca-Cola Hack and Who’s on Hook for Office Cybersecurity,” Bloomberg BNA (January 2018)
- “Cloud Archiving: The Benefits of Super-Fast Email Searches,” Mimecast Blog (December 2017)
- “5 Reasons Your Archive Data Solution Will Do You Wrong,” Mimecast Blog (November 2017)
- “Not Just a Nice to Have. 7 Reasons an All-in-One Cloud Archive Is a Business Necessity,” Mimecast Blog (October 2017)
- “The 5 Biggest Challenges of Mobile Email Management,” Mimecast Blog (September 2017)
- “Scottrade Wins Dismissal of Data Breach Suit,” Westlaw Journal Computer & Internet (July 2016)

Experience

- Developed HIPAA-compliant best practices policies and training for covered employers and providers
- Audited compliance with data privacy and security laws and regulations
- Represented large multinational corporations in data breach investigations
- Defended large pharmaceutical manufacturer in a trade secret case involving alleged theft of clinical data
- Negotiated technology license and use agreements, off-site data storage and security agreements, and data evaluation and manipulation agreement with client vendors
- Counseled clients and provided emergency response services and disclosures with respect to inadvertent disclosures and access to confidential consumer, employee, and customer information
- Defended individuals and executives in response to allegations of actual or potential criminal conduct arising from data breaches and security related issues
- Prosecuted Qui Tam actions in the healthcare industry resulting in the federal government's interventions and recovery of funds against multi-state healthcare providers and medical device manufacturers
- Defended organizations and individuals against False Claims Act litigation brought by the federal government and Qui Tam relators in the construction, healthcare, transportation, and government procurement industries
- Defended healthcare providers, hospitals, and insurance coverage providers in response to claims of alleged HIPAA and state medical privacy law violations
- Represented business claimants in allegations that other businesses and individuals have misappropriated and/or misused proprietary or confidential information
- Engaged in a FINRA investigation arising from a violation of Reg SP, an SEC promulgated privacy regulation
- Represented an international company in prosecuting a theft of trade secrets case relating to its Brazilian operations
- Representations in connection with restrictive terms of use relative to electronic information access, including electronic files and electronic documents
- Counseled clients in connection with electronic document security, including watermarking, glyphs, encryption, and tracking
- Represented businesses and their employees alleged to have engaged in theft of trade secret claims