



Lauren Watson

PARTNER

THE LINK VIRTUAL OFFICE

PHONE: 202.378.2322

EMAIL: LAUREN.WATSON@HUSCHBLACKWELL.COM

WASHINGTON, DC*

PHONE: 202.378.2300

OVERVIEW

Lauren helps organizations develop frameworks to use data and emerging technologies responsibly and confidently, balancing legal obligations with business objectives. As privacy, cybersecurity, and artificial intelligence (AI) become increasingly interconnected, she designs tailored compliance strategies to protect, manage, and leverage data effectively. She practices from Raleigh, North Carolina as a member of our virtual office, The Link.

Lauren counsels clients on a broad range of privacy and technology matters, including electronic monitoring and surveillance, biometric privacy, AI, and automated decisionmaking, and the adoption of global data privacy and security programs. She also advises on privacy compliance initiatives, including the preparation and implementation of privacy notices and policies, data subject rights processes, data governance strategies for the collection, use, sharing, and commercialization of personal information, and negotiation of data protection agreements.

Her experience spans U.S. and international privacy, cybersecurity, and AI laws and regulations, including sector-specific requirements such as the Health Insurance Portability and Accountability Act (HIPAA), the New York Department of Financial Services (NYDFS) Cybersecurity Regulation, and the Washington My Health My Data Act (MHMDA); AI and

Industries

Manufacturing
Technology
Transportation

Services

Artificial Intelligence
California Consumer Privacy Act
Colorado Privacy Act Resource Center
Data Privacy & Cybersecurity
EU Data Protection and Privacy
Fintech
Labor & Employment
Mergers & Acquisitions
State Privacy Laws

automated decisionmaking laws including California's Automated Decisionmaking Technology (ADMT) and risk assessment regulations, the Colorado AI Act, Connecticut AI Responsibility and Transparency Act, Illinois Human Rights Act (as amended by HB 3733), and NYC Local Law 144; U.S. state comprehensive privacy laws, such as the California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act (CCPA/CPRA), Colorado Privacy Act (CPA), Texas Data Privacy and Security Act (TDPSA), Virginia Consumer Data Protection Act (VCDPA), Connecticut Data Privacy Act (CTDPA), and Utah Consumer Privacy Act (UCPA); and international privacy laws, including the EU General Data Protection Regulation (GDPR), United Kingdom General Data Protection Regulation (UK GDPR), and Canada's Personal Information Protection and Electronic Documents Act (PIPEDA).

Lauren also advises clients on cybersecurity incident preparedness and response, helping organizations develop and test incident response plans, conduct tabletop exercises, and navigate all stages of data security incident response, from initial containment and remediation to breach notification obligations and regulatory investigations.

Clients value Lauren's ability to translate complex privacy and technology issues into practical guidance. She works with organizations of all sizes, from established enterprises refining mature privacy programs to startups and growing companies building compliance programs from the ground up, helping them develop the knowledge and processes necessary to identify issues, address routine matters independently, and recognize when strategic legal support is warranted. This collaborative approach allows Lauren to develop lasting relationships with clients and serve as a trusted adviser as their needs and regulatory obligations evolve.

Experience

- Counseled clients on the interplay between state data broker laws and existing comprehensive privacy law obligations (e.g., CCPA/CPRA, VCDPA) where a single data-sharing practice implicated both regimes.
- Negotiated data licensing and data-sharing agreements, including terms addressing permitted use restrictions, downstream compliance obligations, deletion and opt-out honoring mechanics, and liability allocation for regulatory noncompliance by data recipients.
- Partnered with cross-functional legal, HR, technical, and operational teams to guide clients through the adoption of artificial intelligence (AI) technologies, including by providing advice and counsel regarding vendor due diligence and data subject notice and consent requirements, as well as developing internal policies and standards governing the use of AI tools like AI recording and notetaking tools, generative AI (including large language models or LLMs) and machine-vision equipped surveillance instruments.

Experience

- Worked closely with clients operating in both business to business (B2B) and business to consumer (B2C) industries to develop and implement comprehensive international and domestic data privacy compliance programs.
- Navigated clients through web of privacy, biometrics, and automated decision-making technology (ADMT) laws in the U.S. and internationally relating to the use of vehicle telematics, AI-cameras, productivity enhancement tools, and other forms of monitoring and surveillance technologies.
- Negotiated and drafted hundreds of complex privacy and data protection contract terms, including for clients in heavily regulated industries.
- Led clients, including Fortune 500 pharmacy chain, through data breach obligations, including internal incident response and remediation, management of outside forensic and information security experts, and identification and completion of individual and regulatory notifications in relation to incidents involving individuals in all 50 states and overseas.
- Prepared documentation for clients seeking to self-certify to the EU-U.S. Data Privacy Framework, UK extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework.
- Drafted and negotiated data protection agreements for clients in a variety of industries incorporating contract terms mandated by U.S. state comprehensive privacy laws, as well as the European Commission's revised Standard Contractual Clauses and the UK addendum to the same.
- Directed HIPAA Security Assessments and Risk Analyses for covered entities and business associates.
- Assisted major national retailer with development and implementation of Washington State My Health My Data Act compliance program.

Recognition

- *Best Lawyers: Ones to Watch® in America*
 - Labor and Employment Law - Management, 2027
 - Litigation - Labor and Employment, 2027

Education

- J.D., University of North Carolina School of Law
 - *North Carolina Journal of International Law*, Senior Staff Editor
- Visiting Student, University of Oklahoma College of Law
 - American Jurisprudence Award, Cybersecurity Law
 - American Jurisprudence Award, International Law Foundations
- B.A., University of North Carolina at Chapel Hill
 - with distinction

Admissions

- North Carolina
- District of Columbia
- Oklahoma
- U.S. District Court, Eastern District of Oklahoma
- U.S. District Court, Northern District of Oklahoma
- U.S. District Court, Western District of Oklahoma

Community Leadership

- Me Fine Foundation, Board of Directors, Chair

*Lauren works remotely and is licensed in North Carolina, practicing in Raleigh, North Carolina. Contact Lauren via email or phone for in-person/virtual meetings. Use the Washington, DC office address for mail/deliveries only.