About the Author

Rebecca Perry CIPP/US/G
Director of Strategic Partnerships
636.821.2251 | **office**
rperry@jordanlawrence.com

Rebecca has been assisting legal, compliance, privacy and IT executives for over 25 years in the areas of information governance, data mapping, data minimization, records retention and third-party diligence. She is a Certified Information Privacy Professional and a frequent speaker in the privacy community, including sessions with the FTC, Association of Corporate Counsel, Society of Corporate Governance and IAPP KnowledgeNet.

How Can You Begin to Comply Data Privacy & Cybersecurity Regulations?

Since the enforcement of the EU's General Data Protection Regulation (GDPR) began, we've seen a rapid increase in proposals and approvals for data privacy and cybersecurity regulations across the globe. In the United States, the California Consumer Privacy Act (CCPA) has become the template for many other states' privacy laws. Presently, nine other states are considering legislation that closely mimics the structure and language of the CCPA. We can expect to continue to see an uptick in state-specific legislation related to data privacy and cybersecurity until a federal privacy bill is passed.

The recently published 2019 ACC Chief Legal Officers Survey noted that data breaches, regulatory changes, and information privacy top the list of concerns for CLOs in 2019. Notably, Illinois' Biometric Information Privacy Act (BIPA) has been making waves in the legal community since the Illinois Supreme Court determined in the highly publicized Six Flags case that an "aggrieved person" does not have to demonstrate harm to file suit against a company for BIPA violations. Rather the decision notes that "the violation, in itself, is sufficient to support the individual's or customer's statutory cause of action". This landmark decision is impacting over 200 other BIPA cases currently being tried and is causing many companies to re-evaluate their biometric data collection policies and practices. Similarly, a recently proposed amendment to the CCPA (Senate Bill 561) would modify the private right of action for consumers by eliminating the necessity to demonstrate unauthorized access and exfiltration, theft, or disclosure of their non-encrypted or non-redacted personal information.

Failure to adequately identify, address, and minimize risks to personal and sensitive data can result in significant legal and financial harm. U.S. and international regulations and laws require companies to conduct full-scale personal data inventories, resolve issues that are surfaced, and maintain an up-to-date inventory for ongoing compliance and reporting requirements. This is clear in both the regulatory requirements as well as guidance published by regulators and data protection authorities.

You must know where your data is to protect it, delete it, report on it, and produce it. A defensible data inventory identifies where personal data exist, processing activities, transfers, storage locations, access levels, retention periods, and other critical elements. Our clients are often surprised to find where their data exist. For instance, our work with clients on Data Inventories shows that on average, over 75% of records saved in email and over 90% of records saved to shared drives contain personal or sensitive data. On average, our clients find that over half of their records can be appropriately disposed of immediately.

It's easy to get lost in the chaos of slightly varied data privacy and cybersecurity regulations. Developing and maintaining an accurate, up-to-date data inventory doesn't have to be confusing or complicated. Jordan Lawrence helps clarify your obligations, understand the who, what, where, why, and how of your data collection practices and determine which regulations apply to your data, so you can ensure defensible compliance.

About the Author

Rebecca Perry CIPP/US/G
Director of Strategic Partnerships
636.821.2251 | **office**
rperry@jordanlawrence.com

Rebecca has been assisting legal, compliance, privacy and IT executives for over 25 years in the areas of information governance, data mapping, data minimization, records retention and third-party diligence. She is a Certified Information Privacy Professional and a frequent speaker in the privacy community, including sessions with the FTC, Association of Corporate Counsel, Society of Corporate Governance and IAPP KnowledgeNet.