Introduction to the 2025-2026 Edition

There have been many recent developments in the law of data security and privacy, including:

Chapter 1: Electronic Security Risks and the Need for Privacy

- In 2024 over 2800 data breaches occurred with over 1.2 billion victim notices.
- The average cost of a data breach in 2024 has increased from $4 million to 5 million dollars.
- 2024 ransomware cases increased by 15% but over half of the 5,289 attacks occurred in the United States.
- Companies are increasing the usage of web trackers that they can use to profit off of web users as they browse the internet.
- The average cost of a healthcare industry data breach remains around $10 million and are the most costly of data breaches.

Chapter 6: Data Security Statutes

- The Seventh Circuit Court of Appeals in Motorola Solutions, Inc. v. Hytera Communications Corp., 108 F.4th 458 (7th Cir. 2024) allowed a manufacturer to seek extraterritorial damages under the Defend Trade Secrets Act because the foreign competitor defendants marketed products embodying the plaintiff's alleged trade secrets at U.S. trade shows.
- The Eight Circuit Court of Appeals in Jones v. Bloomingdales.com, 124 F.4th 535 (8th Cir. 2024), "join[ed] the overwhelming number of district courts" to hold that plaintiffs lack standing for federal wiretap claims involving the use of session replay technology to capture non-private information about consumers' routine online browsing activities.
- The Ninth Circuit Court of Appeals in U.S. v. Pangang Group Co., 2025 WL 1215487 (9th Cir. Apr. 28, 2025) concluded that the defendants were not eligible for foreign sovereign immunity for alleged trade secret theft because they did not establish a prima facie case for such immunity under federal common law.
- On April 24, 2024, President Joe Biden signed into law the Protecting Americans' Data from Foreign Adversaries Act

of 2024 (PADFAA), which aims to prohibit data brokers from transferring personally identifiable sensitive data of US individuals to foreign adversaries and entities controlled by foreign adversaries.

- On October 2, 2024, the New York State Department of Health adopted new regulations that require hospitals to establish, implement, oversee, and maintain minimum cybersecurity standards to ensure business continuity and protect information systems and nonpublic information from cyber threats.

Chapter 7: Data Privacy Statutes

- The FTC's most recent Privacy & Data Security Update highlights growing concerns around AI, youth privacy, and sensitive data, while renewing its call for comprehensive federal privacy legislation.
- Several new comprehensive state data privacy laws have been enacted across the United States in the past year.

Chapter 8: Civil Litigation

- New case law over the past year has addressed foundational legal questions, such as jurisdiction, in the context of modern technology.
- The FTC has recently increased its efforts to hold companies responsible for weak security practices and repeated data breaches.

Chapter 10: Corporate Security and Privacy Duties, Policies and Forms

- In the past year, organizations around the world have experienced the largest increase in global data breach costs since the COVID-19 pandemic.
- The European Union has formally adopted the EU Artificial Intelligence Act: the world's first comprehensive legal framework for AI.
- Privacy laws have been enacted in twenty states with more states considering passing such legislation.
- The SEC and CISA have offered regulations for the reporting of cyber breaches.
- Artificial Intelligence (AI) continues to offer efficiencies for its use, while also presenting companies and attorneys with numerous issues and challenges.

Chapter 14: Personal Data Protection Laws Around the World

- Over the past year, new data privacy laws (and corresponding Data Protection Authorities) have emerged in several countries worldwide.