PRIVACY & CYBERSECURITY UPDATE

3 Key Trends To Watch

From heightened scrutiny in M&A transactions to significant regulatory changes across the Atlantic and the ongoing fortification of state laws in the US, practitioners must stay informed to navigate these shifts effectively. Here is what you need to know.

-1-

Privacy and Cybersecurity are Moving Center Stage in M&A Transactions

The focus on privacy and cybersecurity diligence in M&A transactions has grown exponentially, regardless of the target industry. Privacy diligence exercises are becoming more nuanced as new state laws come into effect, cyber incidents and vulnerabilities are continuing to make headlines, and companies are navigating an increasingly complex regulatory landscape. Against that backdrop, pre-signing and pre-closing penetration testing and threat assessments are becoming more commonplace, along with special indemnities, closing conditions tied to remediation of security vulnerabilities, and walkaway rights tied to pre-closing data breaches and cybersecurity incidents.

-2-

Signs of Relaxation in Regulatory Frameworks Across the Pond

GDPR Amendments for SMEs

In May 2025, a proposal was introduced to amend the General Data Protection Regulation (GDPR) to relax certain requirements for small and medium-sized enterprises (SMEs) by expanding exemptions under Article 30's record-keeping requirements. The most significant proposed amendment would exempt organizations with fewer than 750 employees from mandatory record-keeping obligations unless their data processing activities are deemed to be "high risk." The proposed changes are targeted, but the scaling back of the GDPR in any way is noteworthy. Does it portend a shift in prioritizing innovation over compliance burden? Too soon to tell.

Data Privacy Brexit

Meanwhile, Data Privacy Brexit is finally happening. After several attempts at passing its own regulatory package, on June 19, 2025, the UK Parliament enacted the UK Data (Use and Access) Act 2025 (DUAA). The DUAA is expressly aimed at decreasing data protection burdens on companies by encouraging innovation and allowing for responsible data sharing to reflect the evolving digital landscape. The DUAA simplifies prior regulations related to cookies, automated decision making, the processing of personal data for certain marketing activities, and international data transfers.

EU Artificial Intelligence Act is Up and Running

First there were rumblings of momentum to delay deadlines. Then there were shifting views coming out of Brussels hinting that the European Commission may be open to scaling back the EU Artificial Intelligence Act amid industry pressure and transatlantic geopolitical economic developments. In the meantime, the Commission has pressed ahead, ticking off the earlier deadlines on its roadmap.

-3-

US Privacy Patchwork Is Being Sewn with Steel

We still have no comprehensive federal privacy or AI laws or regulations in the United States. Nor are we likely to have either any time soon, based on the current federal legislative landscape. Instead, we have 19 comprehensive state privacy laws on the books – our state privacy patchwork – with several slated to take effect in late 2025 and 2026. While the passage of new comprehensive laws slowed in 2025, state legislators have continued to reinforce the patchwork seams with steel. Several states have fortified existing laws with robust privacy-protective amendments.

Colorado: Biometric Data Protections

Colorado imposed heightened protections for the collection and processing of employees' biometric data.

Connecticut: Expanded Privacy Framework

Connecticut made a number of changes to its existing privacy framework, such as expanding the scope of applicability thresholds, broadening the definition of "sensitive data," and requiring controllers to make a statement disclosing whether they collect, use or sell personal data for the purpose of training large language models.

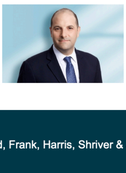
Montana: GLBA Exemption Removal

Montana removed an entity-level exemption for GLBA-covered businesses (but left its GLBA data-level exemption in place).

California: CCPA Amendments

The California Privacy Protection Agency Board finalized its long-awaited amendments to the California Consumer Privacy Act (CCPA) regulations. The final rulemaking package will be sent to the Office of Administrative Law (OAL) to confirm that the updates are in alignment with the CCPA and relevant administrative procedures. Assuming that the OAL approves these updates, the regulations will add, among other things, new requirements covering automated decision-making technology (ADMT), risk assessments and cybersecurity audits. While the ADMT regulations, in particular, reflect a more business-friendly package than initially proposed, businesses subject to the CCPA will have many new obligations to add to their compliance program.

For more information on the latest trends and developments, please contact:



Michael Kleinman
Privacy and Cybersecurity Partner
T: +1.212.859.8476
Michael.Kleinman@friedfrank.com

© 2025. Attorney advertising. Prior results do not guarantee a similar outcome.