MARCH 2026

COVINGTON

Technology Industry Trends and M&A Outlook in the U.S.

Introduction

As described in our earlier blog post, many of today's largest M&A and strategic transactions focus on technologies and functions that enable those technologies – from digital infrastructure and data centers to artificial intelligence (AI). To realize the full potential and maximize business opportunities, strategic technology transactions must reflect careful attention to the dynamic U.S. regulatory landscape. This blog provides an overview of technology trends in privacy, cybersecurity and AI relevant for executing technology-focused M&A and other strategic transactions in the US.

Tech as a regulated sector

At the federal level, the US has not enacted a comprehensive privacy law or industry-agnostic federal law that applies to technologies like AI. However, federal sector-specific laws regulate use of data in certain contexts, such as the Health Insurance Portability and Accountability Act ("HIPAA") and the Gramm-Leach-Bliley Act ("GLBA"). Additionally, there are also nearly two dozen state comprehensive privacy statutes that govern the collection, use, and disclosure of personal data, including personal data used to develop and deploy AI and related technologies. Adding additional complexity, state laws that regulate specific technologies, like AI, can impose further requirements.

Executing a technology-focused M&A or strategic transaction among this patchwork of state laws, therefore, requires understanding how the commercial value in an asset, technology, or business model may be implicated by the regulatory environment.

Key regulatory developments

The U.S. regulatory environment remains dynamic and variable. The Trump Administration has espoused a largely deregulatory agenda to promote AI innovation and adoption, including an executive order aimed at preempting state AI laws. At the same time, and in spite of that pressure from federal policymakers, state lawmakers and regulators continue to prioritize AI and have introduced or advanced hundreds of pieces of legislation focused on regulating AI models and systems. For example, some of these frameworks focus on greater transparency related to interactions with AI systems or content, whereas others focus on safety-concerns related to frontier-size models or use of AI in employment decisions.

Authors

Jayne Ponder
Associate, Washington
+1 202 662 5008
jponder@cov.com

Vanessa Lauber
Associate, New York
+1 212 379 8741
vlauber@cov.com

Clare Mathias
Associate, Boston
+1 617 603 8822
cmathias@cov.com

Kyle Falkner
Associate, Washington
+1 202 662 5840
kfalkner@cov.com

Meanwhile, state legislatures have amended existing state comprehensive privacy statutes and issued regulations under these AI frameworks. Many of these amendments and regulations specifically target the use of personal data related to AI and similar technologies.

Accordingly, while each technology is different, privacy, cybersecurity, and AI regulation play an important role in strategic dealmaking. The table below summarizes some key sources of U.S. regulation on these topics. If a technology is implicated in these standards, consider: (1) can the issue be remediated effectively and efficiently, (2) what is the timeline for doing so, (3) what does good risk allocation look like in the deal (and in particular the risk of regulatory fines or action prior to closing), and (4) are there reputational issues that cannot be contractually allocated, but which can otherwise be mitigated or assumed?

cannot be contractually allocated, but which can otherwise be mitigated or assumed?

Regulatory Area	Examples of Key Sources	Value Impacting Considerations
Privacy	▪ Health Insurance Portability and Accountability Act (HIPAA) ▪ Gramm-Leach Bliley Act (GLBA) ▪ Children's Online Privacy Protection Act (COPPA) ▪ Fair Credit Reporting Act (FCRA) ▪ Section 5 of the Federal Trade Commission Act (FTC Act) ▪ DOJ Bulk Sensitive Data Rule ▪ Nearly two dozen state comprehensive privacy statutes ▪ State consumer health privacy laws ▪ State biometric privacy laws (e.g., Illinois Biometric Information Privacy Act) ▪ State genetic privacy laws	If the technology involves the collection, use, or disclosure of personal data or other data regulated under privacy frameworks, have consumers been provided proper disclosures, are any required contractual terms in place, and have consumers been afforded opportunities to exercise their consumer rights, as required by applicable laws? What representations has the seller made to individuals and third parties regarding personal data and how might these representations impact the potential opportunity?

```
operation == "MIRROR_X":
irror_mod.use_x = True
irror_mod.use_y = False
irror_mod.use_z = False
_operation == "MIRROR_Y"
irror_mod.use_x = False
irror_mod.use_y = True
irror_mod.use_z = False
_operation == "MIRROR_Z"
irror_mod.use_x = False
irror_mod.use_y = False
irror_mod.use_z = True

election at the end -add
_ob.select= 1
er_ob.select=1
ntext.scene.objects.activ
("Selected" + str(modifier
irror_ob.select = 0
 bpy.context.selected_ob
ata.objects[one.name].se

int("please select exactl
```

Regulatory Area	Examples of Key Sources	Value Impacting Considerations
Cybersecurity	■ GLBA Safeguards Rule ■ HIPAA Breach Notification Rule ■ CCPA Cyber Audit Requirements ■ New York SHIELD Act ■ New York Department of Financial Services Cybersecurity Regulation (23 NYCRR 500) ■ 54 state and territorial data breach notification requirements	Does the core technology meet applicable cybersecurity requirements? Does the technology implicate a highly regulated sector, such as health care or financial services, that is subject to enhanced cybersecurity or information security standards? Are there potential risks arising from past cybersecurity incidents, including regulatory penalties, consumer lawsuits, or contractual violations, that may impact the value of the deal? Do current cybersecurity and technology practices align with industry standards such as the NIST? Have the costs and risks of compliance obligations, such as ongoing cyber audit requirements, been factored into the value of the deal?

Regulatory Area	Examples of Key Sources	Value Impacting Considerations
AI	▪ White House AI Action Plan ▪ Ensuring a National Policy Framework for Artificial Intelligence Executive Order ▪ Colorado AI Act ▪ Texas Responsible AI Governance Act ▪ Requirements regarding the use of AI in employment decisions (e.g., NY Local Law 144) ▪ Requirements to disclose training data or AI interactions (e.g., CA AB 2013, CA SB 243, UT SB 149) ▪ Requirements regarding synthetic content (CA SB 942) ▪ California Privacy Protection Agency (CPPA) regulations for automated decision making ▪ Frontier Model requirements (e.g., NY RAISE Act)	Has the technology been developed and deployed in compliance with applicable federal and state law requirements, such as complying with risk management and consumer choice requirements if an AI technology makes sensitive decisions? Is the technology designed to interact with consumers or otherwise generate content the consumers will interact with? Is the technology likely to be used in any “high risk” scenario or to make significant decisions (e.g., employment, housing, lending, healthcare) or does the deal involve a model that would be defined as “frontier” under relevant requirements? Are AI governance policies consistent with industry standards, such as the NIST or ISO/IEC AI frameworks?

Implications for dealmakers

U.S. privacy, cybersecurity, and AI frameworks continue to present a dynamic environment with a meaningful impact on strategic transactions. The execution of successful transactions requires not only a careful assessment of existing and emerging regulatory regimes, but also an understanding of trends in how these laws are evolving.

As we continue in our series, we will consider key U.S. antitrust dynamics and practical insights as to how those influence M&A and other strategic transactions.