

August 4, 2021

## MERGERS &amp; ACQUISITIONS

# Evaluating Privacy and Cybersecurity Risks in Emerging Technology Transactions: Artificial Intelligence and EdTech

By [Sujit Raman, Sharon Flanagan, Michael R. Roberts and Francesca Blythe, Sidley Austin LLP](#)

Global mergers, acquisitions and strategic investments are at a record high, reflecting a worldwide climate for transactions that is unprecedented in both scope and scale. This significant uptick in transactional activity is taking place in a global environment where privacy, data protection and cybersecurity laws and standards are rapidly expanding. These issues are critical to many deals, particularly where the target company deals with consumers' personal data.

A target company's non-compliance with privacy and cybersecurity responsibilities can undermine its financial valuation, as well as its ability to complete a successful sale, an initial public offering or another strategic transaction. Non-compliance can also impact the target company's reputation, as well as customers' confidence in the business. Accordingly, stakeholders not only must carefully monitor regulatory developments in these areas to protect their existing business and investments, but they also must diligently examine target companies for compliance with applicable privacy, data protection and cybersecurity laws and standards when considering new investments in, or acquisitions of, such companies.

Stakeholders must also carefully review transactional agreements (including purchase agreements, disclosure schedules, transition services agreements and data sharing agreements) to ensure that privacy, data protection and cybersecurity laws and standards are appropriately considered in definitions, representations, warranties, indemnities and other key provisions to allow for appropriate risk allocation.

In this two-part article series, we examine U.S., U.K. and E.U. regulatory trends in four key emerging technology sectors that recently have seen vastly increasing amounts of transactional activity. This first installment covers artificial intelligence and education technology transactions, and part two will address biometrics, as well as financial technology and cryptocurrency transactions. Based on our experience assessing the privacy and cybersecurity aspects of several recent transactions in these data-intensive sectors, we outline many of the key issues that stakeholders may wish to consider when evaluating the privacy, data protection and cybersecurity risk profiles of target companies in those industries.

See "[Privacy and Cyber Due Diligence in M&A Transactions](#)" (Mar. 11, 2020).

## Artificial Intelligence and Automated Decision-Making Technologies

Investments in AI and related automated decision-making technologies are surging in numerous sectors. Diligence in this area should focus on the target company's compliance with recent guidance from key U.S., U.K. and E.U. regulators, and should ensure an appropriate allocation of risk between the buyer/investor and the target company.

### Ensure AI-Related Technologies and Products Align With FTC Expectations

During due diligence, stakeholders should evaluate whether the target company's AI-related technologies and products align with the expectations of the FTC, as outlined in public statements, enforcement actions, studies and guidance.

The FTC has long explored the positive and negative impacts of AI, big-data analytics and machine learning technologies on consumers. For instance, in January 2016, the FTC issued a report, "[Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues](#)," which outlined the steps that businesses could take to reduce exclusionary or discriminatory outcomes from their use of big data analytics and machine learning. The FTC has continued focusing on AI and automated decision-making technologies through published statements and blog posts addressing its regulation of AI technologies.

In April 2020, for example, the Director of the FTC's Bureau of Consumer Protection issued a statement, "[Using Artificial Intelligence and Algorithms](#)," which acknowledged the benefits but also warned of the "risks" presented by AI technologies, including "the potential for unfair or discriminatory outcomes or the perpetuation of existing socioeconomic disparities." This April 2020 statement can serve as a helpful roadmap for stakeholders who must evaluate the privacy and security compliance risks presented by target companies' use of AI and automated decision-making technologies. Specifically, the April 2020 statement emphasized that "the use of AI tools should be transparent, explainable, fair and empirically sound, while fostering accountability."

In April 2021, the FTC issued a statement called "[Aiming for truth, fairness, and equity in your company's use of AI](#)." This statement reminded the public about various "important lessons on using AI truthfully, fairly and equitably," including the need (1) to ensure that the data sets a company uses for AI purposes are not missing information from legally protected population groups; (2) to monitor algorithms for discriminatory outcomes; (3) to embrace transparency and independence in a company's use of data; (4) not to exaggerate "what your algorithm can do or whether it can deliver fair or unbiased results"; and (5) to "tell the truth about how you use data."

The FTC's April 2021 statement follows in the wake of notable enforcement actions in connection with AI technologies. For example, enforcement actions in [2016](#) (involving an adultery-oriented dating website's use of fake "engager profiles" to induce potential

customers to sign up for the dating service) and 2019 (involving the sale of fake followers, phony subscribers and bogus “likes” to companies and individuals that wanted to boost their social media presence) focused on companies that were alleged to have used AI tools to interact with, and deceive, customers.

Thus, from a transactional diligence perspective, stakeholders will want to use the FTC’s public actions and statements as guiding principles to assess certain issues, including whether target companies are:

1. using automated tools in a manner that deceives or could mislead consumers;
2. obtaining sensitive data from consumers for use in data sets without sufficient notice or consent;
3. taking steps to validate and revalidate AI technologies to prevent illegal discriminatory practices; and
4. maintaining and implementing reasonable information security safeguards and processes (e.g., access controls) to ensure that they are protecting the data used by AI and automated decision-making technologies.

See “[Maximizing the Benefits of Big Data Within Permissible Bounds](#)” (Aug. 24, 2016).

## Focus Evaluation on Compliance and Non-Biased Algorithms

Stakeholders should evaluate the extent to which the relevant AI and automated decision-making technologies comply with applicable laws and do not deploy biased algorithms that would constitute violations of such laws.

These laws include Section 5 of the FTC Act (if practices may be deemed unfair or deceptive), the Fair Credit Reporting Act (particularly if an algorithm is potentially being used to deny people employment, housing, credit, insurance or other benefits) and the Equal Credit Opportunity Act (if there is a risk of illegal practices, such as using a biased algorithm that results in credit discrimination on the basis of race, color, religion, national origin, sex, marital status, age or because a person receives public assistance).

In addition, stakeholders should consider the applicability of comprehensive U.S. state privacy laws (e.g., California, Virginia and Colorado) to a target company’s businesses and, if applicable, how these laws and their implementing regulations may impact a target company’s use of AI technologies and automated decision-making technologies.

See CSLR’s AI Compliance Playbook series: “[Traditional Risk Controls for Cutting-Edge Algorithms](#)” (Apr. 14, 2021); “[Seven Questions to Ask Before Regulators or Reporters Do](#)” (Apr. 21, 2021); and “[Understanding Algorithm Audits](#)” (Apr. 28, 2021).

## Review Applicable Transactional Agreements

Stakeholders should also review applicable transactional agreements to ensure that their provisions appropriately account for any AI and automated decision-making technologies that may be essential to the deal.

Depending on their risk appetite, parties may seek to revise already defined terms to include AI technologies and assets or, if AI is integral to the deal, may negotiate specific defined terms,

representations and warranties, and indemnities that help appropriately address and shift particular risks related to the AI technologies.

The parties may wish to review transactional agreements to confirm that their provisions account for the sources, security, current and future uses, training and users of relevant AI data sets and technologies. There may also be notice and consent considerations from a privacy perspective related to the AI data sets, as well as issues related to anonymization. For instance, stakeholders may need to consider whether any sensitive personal information (including any protected health information) may be used in training the AI technologies.

In addition, parties will want to determine appropriate look-back periods for the representations and warranties to capture the past, present and anticipated future uses of, and any evolving regulatory standards and risks applicable to, AI technologies. Of course, the intellectual property, privacy/security and corporate/M&A specialists working on the deal should collaborate closely, as AI naturally presents sensitive cross-cutting issues, such as data collection and licensing.

See [“Essential Cyber, Tech and Privacy M&A Due Diligence Considerations”](#) (Aug. 8, 2018).

## Consider E.U./U.K. Privacy Laws

From an E.U./U.K. privacy perspective, stakeholders should diligence key issues, such as the extent to which AI technologies involve solely automated decision making without any meaningful human interaction.

If such technologies have a legal or similarly significant effect on individuals, this type of

processing is restricted under E.U./U.K. privacy laws, and stakeholders should therefore assess whether the process is lawful and whether adequate information has been provided to impacted individuals.

Stakeholders also should assess whether the target company may have made the incorrect determination regarding whether it is providing these AI services as a “processor” or as a “controller,” which will have important implications regarding the legal liability of the provider under E.U./U.K. privacy laws. While a company may be a processor in connection with the provision of the AI services, providers often reserve the right to use the data received from the customer for their own internal purposes, such as to improve models and systems. For these activities, the provider may be acting as a controller and therefore will need to comply with all relevant E.U./U.K. privacy laws (*e.g.*, notice and consent requirements).

It is also important that stakeholders consider the privacy issues related to the quality of the data that the target company is using to train the AI technologies, because the processing of such training data will need to comply with E.U./U.K. privacy laws. Stakeholders should closely examine whether the training data process involves the processing of personal data from individuals without their knowledge.

Stakeholders should also take into account guidance on AI published by regulators at a national level. For instance, the U.K.’s Information Commissioner’s Office has been particularly active in the AI space, and the European Commission published [its draft AI Regulation](#) in April 2021. The European Commission has indicated that it intends to regulate the use of AI in accordance with the



level of risk the AI system presents to fundamental human rights and other key values of the E.U., and stakeholders should monitor regulatory developments in this area.

See [“How to Achieve Trustworthy AI Using the European Commission’s Final Assessment List”](#) (Aug. 5, 2020).

## Education Technology

According to the Association for Educational Communications and Technology, “education technology” or “EdTech” refers broadly to “the study and ethical practice of facilitating learning and improving performance by creating, using and managing appropriate technological processes and resources.” Given the increasing demand for remote education, transactional activity in the EdTech sector has continued to increase at a rapid pace.

### Assess Applicability of Laws and Whether They Are Properly Addressed

During due diligence, stakeholders should assess the applicability of privacy and security-related laws and regulations to the target company, as well as to its EdTech business practices and vendors. These laws and regulations include the Family Educational Rights and Privacy Act, state laws relevant to education privacy (e.g., California’s Student Online Personal Information Protection Act) and Children’s Online Privacy Protection Act (COPPA).

Stakeholders should then review and revise the transactional agreements to ensure applicable U.S. federal and state laws, E.U./U.K. laws and regulatory considerations are sufficiently

addressed in the agreements’ provisions, including any defined terms, representations, warranties and indemnities.

With respect to COPPA, stakeholders should assess whether the target company has maintained a COPPA compliance program, including any participation in the COPPA Safe Harbor Program; whether it has received any complaints regarding compliance; and whether its process for obtaining verifiable parental consent complies with the applicable law and rules. Additionally, stakeholders should confirm the age range of individuals from whom a target company may be collecting personal data, as certain laws classify minors with respect to specific age thresholds and, therefore, a target company may be covered by some, but not all, of the laws and standards relevant to minors’ data.

While parties may prefer simply to revise defined terms to incorporate such laws and regulations, specific representations and warranties and indemnities may be helpful to track compliance and appropriately shift risk in the transactional agreements based on the target company’s obligations, business practices and due diligence responses.

See [“Far-Reaching Google and YouTube Settlement Offers COPPA Compliance Lessons”](#) (Sep. 18, 2019).

### Consider Children’s Data in the Context of E.U./U.K. Laws

From an E.U./U.K. perspective, due to the sensitive nature of children’s data, stakeholders should examine the target company’s compliance programs for handling such data and for obtaining consent regarding its collection, in accordance with the GDPR and with member-state requirements.

Stakeholders should determine the extent to which any EdTech product or service constitutes the offering of “information society services likely to be accessed by children” because, like COPPA, E.U./U.K. privacy laws include specific requirements with regard to the form of consent obtained for the use of such personal data. However, unlike COPPA, which imposes certain requirements on operators of websites or online services directed to children under 13 years of age, the GDPR requires that parental consent be obtained for all information services offered to children. Stakeholders should also consider which party acts as a data controller because it is the controller’s sole responsibility to make reasonable efforts to obtain and verify the required consent.

*Sujit Raman is a partner in Sidley’s privacy and cybersecurity group, with a wide-ranging practice spanning government investigations and litigation, data protection, information security and management, and cyber governance and preparedness. Before joining the firm, Raman served as Associate Deputy Attorney General at the DOJ where he assisted the Attorney General and Deputy Attorney General in their oversight of the nation’s cyber-related criminal and national security investigations and prosecutions, and led DOJ’s policy formulation in a number of critical areas,*

*including cybersecurity, cross-border data transfers and protection, 5G/supply chain security, and emerging technologies such as facial recognition, cryptocurrency and encryption. He is based in Sidley’s Washington, D.C. office.*

*Sharon Flanagan is a partner in Sidley’s M&A practice and serves as a member of the firm’s management committee, executive committee and its global life sciences leadership council. She represents companies in a broad range of M&A transactions, securities offerings and corporate governance matters, with a particular focus on life sciences/healthcare and technology industries. She serves as managing partner of Sidley’s San Francisco office.*

*Michael Roberts is an associate in Sidley’s privacy and cybersecurity practice, advising clients on regulatory, compliance and transactional matters related to data privacy, cybersecurity and data protection. He is based in the firm’s New York office.*

*Francesca Blythe is a senior associate in Sidley’s privacy and cybersecurity practice, advising international clients on a wide range of data protection, privacy and cybersecurity issues, with a focus on certain key industries including life sciences, asset management and private equity, payments, technology, e-commerce and manufacturing. She is based in the firm’s London office.*