BRACEWELL

INSIGHTS

President Biden Signs Executive Order that Likely Will Lead to Greater Scrutiny of Data Privacy in Corporate Transactions

July 12, 2021

*By: **Lucy Porter** and **Matthew G. Nielsen***

On July 9, 2021, President Biden signed an ***Executive Order*** titled "Promoting Competition in the American Economy." Data privacy regulations are among 72 other initiatives in the Executive Order aimed at increasing competition through the issuance of agency rules and enforcement. Following other federal and state lawmakers, this Executive Order is the latest attempt to address how companies use and collect consumer data.

Under this Executive Order, the FTC is directed to start what could be a years-long rulemaking process to strengthen consumers' data privacy. First, the Order looks to safeguard the acquisition of consumer data through mergers and other corporate transactions. The Order sets a policy "to enforce antitrust laws to meet the challenges posed by new industries and technologies, including the rise of the dominant Internet platforms, especially as they stem from serial mergers, the acquisition of nascent competitors, the aggregation of data, unfair competition in attention markets, the surveillance of users, and the presence of network effects." Second, the Order directs the FTC to establish new rules to address "unfair data collection and surveillance practices," particularly in the tech industry. Through this Executive Order, President Biden has given FTC Chair Lina Khan, a Big-Tech critic and privacy advocate, the green light to do what Congress has been unable to do: institute comprehensive, federal data privacy rules.

The Order also directs the Consumer Financial Protection Bureau (CFPB) to issue rules allowing for data portability of consumers banking data. While most of the work relating to technology in the order will happen outside of the executive branch, the order does establish the White House Competition Council to promote these policies.

Bracewell will continue to follow the developments in data privacy stemming from this Executive Order. However, in the meantime, companies should consider taking proactive steps to ensure that they have robust and appropriate data-privacy procedures in place to address this increasingly regulated area, including:

- Identifying and reviewing applicable laws– data privacy compliance has become increasingly complex due to the patchwork of laws and regulations across the country and world;

- Conducting targeted due diligence of privacy compliance in the merger and acquisition process – the rapid expansion of data security and privacy regulations harbors the potential for substantial liability. Whether a target company collects employee data, client data, consumer data, or a combination of the three, an analysis of how data is collected, processed, and protected is critical to the due diligence process;

- Conducting a risk assessment and gap analysis – think about how data privacy affects your business and consider whether current controls and procedures are effective at adhering to the privacy laws that affect your company; and

- Training employees and other stakeholders – often, privacy laws have surprising applicability throughout organizations. For example, non-healthcare organizations that perform certain functions that require the use of PII are also subject to the Health Insurance Portability and Accountability Act (HIPAA), which requires employee training to protect the privacy of patients' PII. The Federal Acquisition Regulations (FAR) also requires federal contractors to train employees on protecting sensitive information. Educating employees on how privacy laws affect areas within their responsibility is key to an effective program.