WILLKIE

CLIENT ALERT

One Month In: What We Know About the Trump Administration's Policies on AI, Privacy, and Cybersecurity

February 24, 2025

AUTHORS

Daniel K. Alvarez | Laura E. Jehl | Susan E. Rohol

Last Thursday marked one month since the Trump Administration took office, and in that time the Administration has taken a number of steps on key issues related to artificial intelligence ("AI"), privacy, and cybersecurity. These have included:

- Direct action, such as the rescission of the Biden Administration's AI Executive Order and its replacement with a new AI Executive Order, as well as announcements from the Federal Trade Commission ("FTC") and the Securities and Exchange Commission ("SEC") of new enforcement priorities;
- Indirect action, specifically the deep cuts to agencies like the Consumer Financial Protection Bureau ("CFPB"), the Cybersecurity and Infrastructure Security Agency ("CISA"), the Privacy and Civil Liberties Oversight Board ("PCLOB"), and the National Institute of Standards and Technology ("NIST") that are likely to have implications for policymaking and rulemaking activities related to privacy, cybersecurity, and AI; and

- Inaction, particularly in the case of the Department of Justice's ("DOJ") Bulk Data Transfer Rules, which will usher in sweeping new compliance obligations for many companies, particularly those working with Chinese persons or entities.

In this Client Alert, we highlight the steps taken by the Administration at these key agencies, and what they may mean for companies moving forward.

- **White House Shifts U.S. Government Approach on AI.** In one of his first official acts upon re-entering the White House, President Trump signed an Executive Order rescinding numerous Biden-era executive orders, including the Biden Administration's AI Executive Order, signaling a different policy approach to AI. Three days later, the President signed a second Executive Order focused on "enhancing America's AI leadership." In the second Executive Order, the President directed agencies "to revise or rescind all policies, directives, regulations, orders, and other actions taken under the Biden AI order that are inconsistent with enhancing America's leadership in AI." The second Executive Order also directed the development of an AI Action Plan. Subsequent statements by Vice President Vance at the AI Action Summit in Paris and other key Administration officials reaffirmed that the Administration's focus is on unleashing AI innovation via deregulation and not on combatting the potential downsides of the technology.

- **DOJ's Bulk Data Transfer Rules.** One of the most notable decisions by the Administration thus far is something it has *not* done—that is, not delaying or freezing the effective date of the DOJ's Bulk Data Transfer Rules. These rules, which originated with a Biden Administration Executive Order, prohibit or restrict (depending on the type of transaction) U.S. persons from knowingly engaging in "covered data transactions"—including data brokerage, investment, employment, or vendor transactions—that involve a "country of concern" (e.g., China) or a "covered person" (e.g., a Chinese citizen or China-domiciled company), and require companies to establish a broad due diligence and compliance program to monitor for and prevent such transactions. The rules were published in the Federal Register on January 8, 2025. They come into effect on April 8, 2025, except for the due diligence and compliance program requirements, which come into effect on October 6, 2025.

  There was reason to believe that the new Administration would want to review the rules before they went into effect. That belief was seemingly confirmed when, on Inauguration Day, President Trump signed the Regulatory Freeze Executive Order, which directed agencies to, among other things, "consider postponing . . . any rules that have been issued in any manner but have not taken effect, for the purpose of reviewing any questions of fact, law, and policy." Given the timing of the rules' adoption, the costly implementation requirements for companies, and the potential for civil or criminal penalties for noncompliance, the rules seemed like a prime candidate for review. However, the DOJ has made no statements suggesting a delay of the effective date of the rules. Given how quickly the DOJ moved to address other enforcement priorities after Attorney General Pamela Bondi was confirmed, and the hardline stance on trade with China being taken by the Administration, we now expect the rules to remain unchanged. The upshot is that any delay or relief companies may have been hoping for may not be coming, and they should take steps to be in compliance by April 8, 2025.

- **FTC Shifts Focus From Commercial Surveillance and Privacy to Tech Censorship.** At the FTC, new Chair Andrew Ferguson took a number of swift actions that signal a different direction than that of prior Chair Lina Khan. Of particular note, Ferguson removed from the list of proceedings open for public comment the FTC's "commercial surveillance" rulemaking. In this proceeding, opened in 2022, the FTC proposed to issue "trade regulations" that would have imposed express rules related to the collection, use, and disclosure of personal information by companies in the U.S., including data minimization and data security obligations that many thought would cripple the advertising industry. The FTC's removal of the proceeding from its list of open proceedings indicates that there are no current plans to move forward with the proposed rules. Then, on February 20, the FTC announced a new and very different enforcement focus: tech censorship. Specifically, the FTC issued a Request for Information (RFI) that called on consumers and employees of technology companies to submit information and examples where technology platforms have harmed consumers by banning users or otherwise restricting access to content. According to the RFI, "FTC staff is interested in understanding how consumers have been harmed—including by potentially unfair or deceptive acts or practices, or potentially unfair methods of competition—by technology platforms that limit users' ability to share their ideas or affiliations freely and openly."

- **SEC's New Cyber Unit.** On February 20, 2025, the SEC announced "the creation of the Cyber and Emerging Technologies Unit (CETU) to focus on combatting cyber-related misconduct and to protect retail investors from bad actors in the emerging technologies space." This new unit will replace the former Crypto Assets and Cyber Unit, which was a key component of former SEC Chair Gary Gensler's expansion of the SEC's role in policing the cybersecurity practices of regulated entities such as public companies and registered investment advisors. Among the issues highlighted as within the CETU's purview, the SEC's release included "Regulated entities' compliance with cybersecurity rules and regulations." The creation of the new unit strongly suggests a reversion to pre-Gensler priorities with respect to cyber enforcement.

- **CFPB Rulemakings on Pause.** The CFPB is among the agencies that have seen the most upheaval in the first month of the Trump Administration. President Trump appointed the head of Office of Management and Budget, Russell Vought, to serve concurrently as the acting Director of the CFPB, and reportedly one of Vought's first actions was to issue a set of directives for employees that included ceasing all stakeholder engagement, pausing all pending investigations and enforcement actions, refraining from approving or issuing any proposed or final rules, and suspending the effective dates of all final rules that have been issued or published but that have not yet become effective. While the agency has not made any official announcements about specific rulemakings, a general pause on all rulemaking activities currently in process at the CFPB would affect proposed rules related to data brokers, open banking standards, and the Fair Credit Reporting Act.

- **CISA and NIST Layoffs.** The new Administration's aggressive push to cut the federal workforce has not spared CISA, the division of the Department of Homeland Security tasked with protecting the nation's cybersecurity and critical infrastructure, or NIST, a nonregulatory agency that is part of the Department of Commerce and is responsible for crafting critical technology standards, including cybersecurity and privacy best practices. At CISA, the focus has been on eliminating roles and resources related to fighting foreign

influence in U.S. elections, bolstering election security and controlling the spread of disinformation. NIST is expected to see cuts of over 500 employees, many of whom are viewed as technical leaders and employees at the AI Safety Institute. Cuts at either of these agencies are likely to slow down key policymaking activities, such as CISA's efforts to adopt incident reporting rules under the Cyber Incident Reporting for Critical Infrastructure Act, and NIST's efforts to update the Cybersecurity and Privacy Frameworks.

- **PCLOB Changes Create Uncertainties for the U.S.-E.U. Data Protection Framework.** The PCLOB is an agency to which many companies have very little exposure—and of which some may never have heard—but which has an outsized and significant impact on transfers of personal data between the E.U. and U.S. The PCLOB is responsible for overseeing U.S. surveillance practices, and plays a key role in the E.U.-U.S. Data Protection Framework ("DPF") by assuring that civil liberties are appropriately considered in the course of any data- and intelligence-gathering undertaken by the U.S. government. On January 27, however, the Trump Administration dismissed the three Democratic PCLOB members, leaving the agency without a quorum, just as the DPF's adequacy decision was making its way through European courts. The sidelining of the PCLOB has cast significant doubt over the continued viability of the DPF, at least in the short and medium term, and has raised concern that the DPF may be invalidated, once again throwing the legality of transatlantic data transfers into limbo.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez	**Laura E. Jehl**	**Susan Rohol**
202 303 1125	202 303 1056	310 855 3172
dalvarez@willkie.com	ljehl@willkie.com	srohol@willkie.com

WILLKIE

BRUSSELS CHICAGO DALLAS FRANKFURT HOUSTON LONDON LOS ANGELES MILAN
MUNICH NEW YORK PALO ALTO PARIS ROME SAN FRANCISCO WASHINGTON