

DOJ Poised To Pounce On Data Security Violators

By **Phillip Bantz**

Law360 (July 11, 2025, 5:35 PM EDT) -- Companies and individuals that are not yet in compliance with the U.S. Department of Justice's sweeping, complex new national data security program should expect to face probes and potentially enforcement actions sooner than later, experts say.

The DOJ's National Security Division paused enforcement of the program from April 8 through July 8, giving a bit of breathing room to companies that were making good faith efforts to comply with the rule, which aims to prevent the sharing of Americans' sensitive data with foreign adversaries including China and Russia.

But that doesn't mean the government wasn't watching for violators and building the foundations for enforcement actions during the reprieve.

"So it could be the case that they have something ready to go in the near future," G. Scott Hulse, a partner at Barnes & Thornburg LLP and former high-ranking DOJ official, told Law360. "Enforcement actions before the end of this calendar year are entirely plausible."

The program is one of the few Biden-era executive orders that have not been tabled under the second Trump administration, highlighting the bipartisan priority of protecting sensitive U.S. data while also signaling the future focus of white collar enforcement.

"This is part of a broader thread where the government seems to be attempting to align white collar enforcement, at least to a large degree, with national security," Hulse said.

The DOJ announced in an April 11 memo that the threat of foreign adversaries collecting and weaponizing U.S. data had become "increasingly urgent, and ensuring prompt compliance with the [program's] requirements is critical to addressing the administration's priorities and stopping the flow of U.S. sensitive personal data and government-related data to countries of concern."

The program carries civil and criminal penalties, including up to 20 years in prison and a \$1 million fine, for companies and individuals caught transferring bulk "sensitive personal data" — including genomic, biometric, personal health, geolocation and financial — to foreign adversaries.

"The DOJ probably won't seek indictments tomorrow, but you can expect voluntary requests for information and subpoenas to be issued soon," Andrey Spektor, a partner at Norton Rose Fulbright and a former federal prosecutor in New York, told Law360 in an email.

"This is top of mind for [national security] prosecutors, and it aligns with some of the recent cases it has brought," he added.

For example, the DOJ on June 30 announced a sprawling enforcement action in an alleged North Korean government scheme involving stealing sensitive data from U.S. employers, including protected military technology. The U.S. government has also criminally charged a Chinese national accused of stealing proprietary data from Google related to artificial intelligence technology.

"There are plenty of white collar and national security prosecutors and federal agents whose work has shifted away from some of the traditional areas of enforcement," Spektor said. "They will see this [program] as a fresh avenue to pursue."

The DOJ has already been poking around for potential violations while also fielding questions from outside counsel for companies seeking more information on the scope of the program, according to Spektor, who cited anecdotal evidence of the activity.

"Prosecutors often take pride in bringing cases that are the first of their kind, and I would not be surprised if they already have some potential targets in mind," he noted.

The DOJ is looking for violations that are intentional or "willful," which can be a high standard for the government. But it might not be such a tall hurdle here because of the extensive guidance that has been issued on the program, according to some experts.

"The government has laid out the steps to compliance pretty clearly and that's going to make it more difficult for folks out of compliance to argue they were unaware or not knowingly violating this rule," said Elizabeth McEvoy, a member of Epstein Becker Green who focuses on white collar and compliance matters.

"Delays in addressing noncompliance or ignoring noncompliance at the start is the type of evidence the government will come back for and try to use for willful violations down the road," she added.

McEvoy told Law360 she expected to start seeing government inquiries about potential program violations within "at least the next month."

Enforcement actions under the program could begin bubbling up within the "next year or so" as the government seeks to make examples out of violators, according to Kate M. Growley, a partner at Crowell & Moring LLP who has been following the program's development.

"When presented with a set of facts exemplary of the kind of corporate behavior that this rule is intended to prevent, it's likely the DOJ will aggressively pursue that in order to demonstrate to the rest of the industry that they should be taking this very seriously," she said.

--Additional reporting by Allison Grande, Julie Manganis and Bonnie Eslinger. Editing by Alanna Weissman and Kelly Duncan.