BRACEWELL

INSIGHTS

Beyond Whistleblowing: Additional Highlights From the Department of Justice at the 2024 ABA White Collar Conference

March 27, 2024

*By: **Seth D. DuCharme**, **Mark Hunting** and **Margaret B. Beasley***

As ***we wrote earlier this month***, the Department of Justice (DOJ) made significant news at the recent American Bar Association White Collar Conference. But the Department didn't stop at announcing its pilot whistleblower incentive program — Deputy Attorney General Lisa Monaco, Acting Assistant Attorney General for the Criminal Division Nicole Argentieri and Assistant Attorney General for National Security Matthew Olsen, highlighted several other areas on which the Department is focused:

- Stiffer penalties for Artificial Intelligence (AI) facilitated violations
- Stiffer penalties for recidivism
- Clarification of the Foreign Extortion Prevention Act (FEPA)
- Sale of US citizens' data to certain foreign parties

Below, we discuss just what these priorities will mean for companies in the year ahead.

Addressing AI

Building on her ***recent speech*** at Oxford University regarding the promise and peril of AI, Monaco discussed the Department's efforts to address this growing threat. "All new technologies are a double-edged sword," she said, "but AI may be the sharpest blade yet. It holds great promise to improve our lives — but great peril when criminals use it to supercharge their illegal activities, including corporate crime."

The Department has long used sentencing enhancements to seek increased penalties for criminals whose conduct presents especially serious risks to their victims and to the public at large, such as increased penalties for use of firearms or other dangerous weapons. Observing the danger of AI being used as such a weapon, Monaco announced the Department's intent to adopt a similar approach in this realm as well. Specifically, where AI is deliberately misused to make a white-collar crime significantly more serious, prosecutors will be seeking stiffer sentences for individual and corporate defendants alike.

Relatedly, Monaco said that the Department now expects companies to proactively address the threat of AI through their compliance programs. In all corporate resolutions, prosecutors assess a company's compliance program — whether it is both designed and empowered to mitigate the company's most significant risks. Additionally, because misuse of AI is now a serious risk for many businesses, the Department will expect compliance programs to specifically address that risk. To that end, Monaco directed the Criminal Division to incorporate assessment of disruptive technology risks — including risks associated with AI — into its guidance on Evaluation of Corporate Compliance Programs. Monaco herself is embarking on an initiative called "Justice AI" — a series of convenings with stakeholders across industry, academia, law enforcement and civil society — to address the impacts of AI.

Corporate Recidivism

In 2023, the DOJ made clear that it would account for a company's criminal, civil and regulatory history when considering the appropriate resolution of an enforcement action. Monaco emphasized that a history of misconduct matters because "penalties exist, in part, to deter future misconduct. They're not the cost of doing business." She rejected the idea that past penalties should serve as precedent, saying that they are only a reference point, but "when a company breaks the law again — and it's clear the message wasn't received — we need to ratchet up the sanctions." For example, when ***Ericsson*** violated its 2019 Deferred Prosecution Agreement (DPA), the Department refused to resolve the case in 2023 for anything less than a corporate guilty plea and fine amount that includes the elimination of cooperation credit originally awarded pursuant to the DPA. Monaco also highlighted the Department's willingness to craft unique remedies, citing ***Teva Pharmaceuticals***: in 2016 Teva resolved a Foreign Corrupt Practices Act violation with a DPA, and when the company faced investigation for price fixing in 2023 the DOJ — for the first time ever — made specific performance a part of the remedy by requiring the company to sell off an entire product line, a novel approach tailored to the company's unique circumstances.

"If your company has had a recent brush with the law, now is the time to invest — and reinvest — in your compliance programs," Monaco said; "I can assure you the price of committing another violation will be far higher than the cost of preventing one."

FEPA Update

Late last year, Congress enacted the ***Foreign Extortion Prevention Act*** (FEPA) to complement the Foreign Corrupt Practices Act (FCPA). FEPA criminalizes the "demand" side of foreign bribery by specifically making it illegal for foreign officials to demand or accept bribes from any United States citizen, company or resident in exchange for obtaining business.

Perhaps anticipating, or responding to, ***concerns*** about international comity, Argentieri said the Department "appreciate[s] the sensitivities of prosecuting a foreign government's officials." She noted that prosecutors in the FCPA Unit and the Kleptocracy Initiative in the Money Laundering and Asset Recovery Section are very experienced at handling these sensitive matters, having investigated and prosecuted foreign bribery cases spanning the globe under other statutes such as the FCPA. Accordingly, Argentieri announced revisions to the Justice

Manual codifying the policy that the DOJ will handle FEPA cases the same way it has treated FCPA cases — with centralized supervision by the Fraud Section, working in partnership with US Attorneys' Offices across the country.

Data Protection

As head of the Department's National Security Division, Olsen emphasized the increasing threat from nation-states and predicted continued focus on these malign actors through the use of any tool available — including financial sanctions, export controls and prohibitions on foreign investments in the United States. He also highlighted a new tool: ***Executive Order 14117*** on "Preventing Access to Americans' Bulk Sensitive Data and United States Government-Related Data by Countries of Concern" (the EO). Olsen explained that Department has long focused on preventing threat actors from stealing data through the proverbial "back door," but this EO "shuts the front door" by denying countries of concern access to Americans' most sensitive personal data.

Signed into law on February 28, 2024, the EO ***authorizes the Attorney General*** to prevent the large-scale transfer of Americans' personal data to countries of concern and provides safeguards around other activities that can give those countries access to Americans' sensitive data. To that end, the DOJ released an ***Advance Notice of Proposed Rulemaking*** to provide additional details on the proposed rules and to provide notice and solicit comment from the public. Olsen emphasized that his division wants to work closely with the industry in developing the regulations, noting that companies are on the front line for these issues and, consequently, protecting national security.

The EO defines sensitive personal data broadly to include personal identifiers, geolocation and related sensor data, biometric identifiers, human 'omic data (*i.e.*, data generated from humans that characterizes or quantifies human biological molecules or metabolic data), personal health data, personal financial data, or any combination thereof, though what types of data specifically are captured by these categories is not fixed by the EO and will be established in the regulations implementing the EO. The anticipated countries of concern are China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba and Venezuela.

Though it will take months to develop and implement the policy, Olsen admonished companies to know their data, know where their data is going, know who has access to the data and know where the data will end up — *now*.