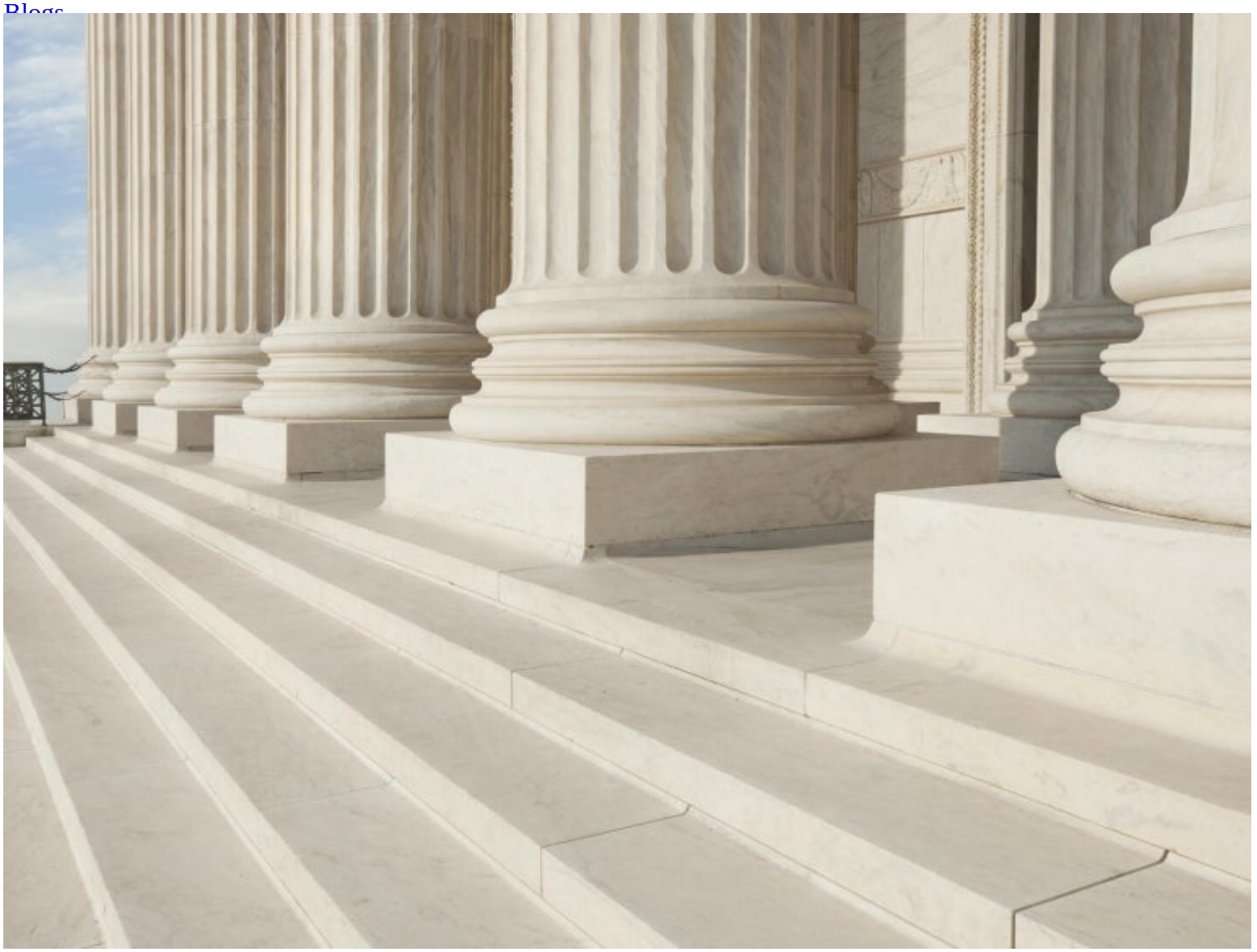

Last week, DOJ's Assistant Attorney General Leslie Caldwell took to the Justice Department's blog to rally support behind recent White House proposals that would bolster law enforcement tools for prosecuting those who create, sell or advertise malicious "spyware."

Spyware refers to software that allows users to surreptitiously intercept communications on their victims' electronic devices such as smartphones and computers. Although prosecutors in the Eastern Division of Virginia recently brought criminal charges against a spyware seller—a case DOJ characterized as the first of its kind—Caldwell states that prosecutorial efforts have been hamstrung by an inability to seize criminal proceeds resulting from sales of spyware, as well as an inability to utilize money laundering charges to go after those who transfer funds across multiple overseas accounts in order to conceal profits from criminal spyware sales. According to Caldwell, the makers and sellers of illegal spyware often reside outside of the United States, and

the millions of dollars of profit they earn is typically concealed via fund transfers through overseas accounts. While prosecutors would generally seek to use money laundering charges in such cases, the spyware statute is not listed as a predicate offense in the money laundering statute. Consequently, the White House proposal adds violations of the spyware statue to the list of money laundering predicate offenses. Similarly, Caldwell indicates that U.S. prosecutors are unable to seek disgorgement of proceeds from illegal sales of spyware, because current law does not authorize the forfeiture of proceeds from the sale of spyware. The White House proposal would expand the statute to include forfeiture of proceeds from the sale of spyware (and property used to facilitate the crime). Although not specifically highlighted in Caldwell's blog post, the White House proposal also seeks to target organized crime groups that utilize cyber attacks by amending the definition of "racketeering activity" under the federal RICO statute to include felony computer fraud as defined under 18 U.S. 1030 ("Fraud and Related Activity in Connection with Computers"). Federal prosecutors have already found some success in using the RICO statute to prosecute cybercrime, but the White House proposals are expected to bolster DOJ's ability to charge members of organized criminal groups engaged in computer network attacks and related cybercrimes.

Explore more in

White Collar & Investigations
Blog series

White Collar Briefly

Drawing from breaking news, ever changing government priorities, and significant judicial decisions, this blog from Perkins Coie’s White Collar and Investigations group highlights key considerations and offers practical insights aimed to guide corporate stakeholders and counselors through an evolving regulatory environment.

View the blog