CLIENT ALERT

Federal Trade Secret Reform Continues With Two New Attempts to Improve Protection

July 22, 2013

In the wake of a 140-page White House report presenting a national strategy to reduce trade secret theft, Congress continues to show interest in refining federal trade secret law to meet the challenges of the internet age. Two bills potentially impacting a company's ability to protect its trade secrets have been introduced. The first, "Aaron's Law Act of 2013," seeks to resolve the Circuit split under the Computer Fraud and Abuse Act (CFAA) such that federal trade secret protection would not apply to the use of electronic information in violation of the employer's computer policies or a website's terms of usage alone. The second, "Private Right of Action Against Theft of Trade Secret Act of 2013" (PRATSA), seeks to create a private right of action under the Economic Espionage Act (EEA), which is presently limited to criminal prosecutions. These efforts reflect a continuation of efforts in the prior Congress to address these issues in a way that strengthens federal protection against industrial espionage without displacing state trade secret law.

Resolving the Circuit Split Under the CFAA

Courts have been struggling with language in the CFAA that creates liability for computer fraud based on "access without authorization" to protected computer systems. The Fifth, Seventh, and Eleventh Circuits interpret that phrase to permit employers to pursue employees who violate computer use policies under the CFAA. Critics have complained that this reading of the CFAA effectively turns run-of-the-mill employment disputes into federal cases under a statute meant to address computer hacking. The Ninth Circuit and several district courts have endorsed a narrower view, holding that an electronic intruder must circumvent a physical or technological barrier, not merely a policy, to be liable under the CFAA. The proposed amendment to the CFAA would codify the more restrictive Ninth Circuit view and thereby reserve for state law employee computer policy violations.

Representative Zoe Lofgren (D-CA) introduced H.R. 2545. Senator Ron Wyden (D-OR), author of the Senate companion bill, said that he seeks to limit the definition of "access without authorization" under the CFAA to gaining unauthorized access to information by "circumventing technological or physical controls such as password requirements, encryption, or locked office doors." Wyden explains on his website that "hack attacks such as phishing, injection of malware or keystroke loggers, denial-of-service attacks, and viruses would continue to be fully prosecutable under strong CFAA provisions" that the bill would not modify.

Opponents of the bill such as Ted Molino of BSA The Software Alliance, an association of software companies fear that the bill is "out of step with the technology innovations driving today's economy" because new technical protection measures adopted by companies would "reverse a trend that has contributed the growth of cloud computing, software as a service, and on-demand support." "Everyone agrees" says Molino, "that lying about your age on Facebook shouldn't be a felony." However, in the absence of a more comprehensive and effective federal law to combat growing trade secret theft, some like Molino fear that this amendment alone would encumber companies' ability to fight trade secret theft by taking one arrow out of their quiver.

A Federal Civil Cause of Action Under the EEA

To address that issue, Representative Lofgren has also introduced PRATSA, which provides a federal civil cause of action for trade secret theft by amending the EEA, which is presently only a criminal statute. This bill is similar to a bill that was proposed last year to create a federal cause of action under the EEA. Unlike that effort, however, which would have created a stand-alone civil claim and a comprehensive set of remedies such as rights to attachment and injunctive relief, exemplary damages, and attorneys' fees for violations, PRATSA only creates a private right of action for violations under the existing EEA provisions. PRATSA does so by adding two subsections to 18 U.S.C. Section 1832:

> (c) Any person who suffers injury by reason of a violation of this section may maintain a civil action against the violator to obtain appropriate compensatory damages and injunctive relief or other equitable relief. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage.
>
> (d) For purposes of this section, the term 'without authorization' shall not mean independent derivation or working backwards from a lawfully obtained known product or service to divine the process which aided its development or manufacture.

Though the current bill does not create a new standalone misappropriation claim, it could significantly augment a company's legal options for protecting trade secrets. Violations of the EEA, including the knowing and intentional theft of trade secrets, would be actionable by private parties in federal court. This is important because the EEA explicitly applies to extraterritorial conduct if the offender is either a U.S. citizen or permanent resident alien, or an organization organized under U.S. law. And several commentators have noted that state trade secret law is often ineffective against misappropriators who flee the country.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Mark A. Klapow
Partner – Washington, D.C.
Phone: +1 202.624.2975
Email: mklapow@crowell.com