CARLTON FIELDS

Rule Change Would Let Law Enforcement Access Computers Remotely Regardless of Location

June 17, 2016

The Supreme Court recently adopted a proposed change to Rule 41 of the Federal Rules of Criminal Procedure that would allow a federal judge to issue warrants authorizing government agents to access computers located in any jurisdiction, possibly even outside the United States, when the computer's location is unknown, and "to search electronic storage media and to seize or copy electronically stored information" from such a computer. This proposal is a departure from restrictions that typically limit a judge's authority to authorize search warrants to within the judge's jurisdiction, and it would effectively allow a federal agent to remotely access information on any computer regardless of its location. The proposal takes effect December 1, 2016, unless Congress acts to modify, reject, or defer it before then. The FBI and DOJ have long advocated for such a change to Rule 41, citing difficulties in performing their enforcement duties in the face of increasingly prevalent technologies that can be used to conceal one's identity online. However, some fear the proposal is too expansive and potentially unconstitutional. For example, Senator Ron Wyden of Oregon said "this rule change could potentially allow federal investigators to use one warrant to access millions of computers, and it would treat the victims of the hack the same as the hacker himself." Indeed, the proposed rule change poses

security and privacy risks for legitimate businesses and individuals, particularly those who might be unsuspecting victims of malicious attacks. The proposal's broad language seems to give law enforcement the authority to access and seize information from computers that might be behind proxies or firewalls (which legitimate businesses commonly use for both security and performance purposes) and computers that might be part of a botnet (a network of computers infected by malware and under the control of a malicious third party without the owners' knowledge). Given that it is unclear whether and how law enforcement intends to protect the confidential information of innocent parties, this rule change poses real risks for both individuals and businesses. For example, information seized by the government under the new rule could potentially be disclosable through FOIA requests, and if such information included trade secrets or confidential personnel files, that could mean liability – or at least bad publicity – for the individuals or businesses from whom the information was taken. Given the stakes at issue, it will be important to monitor whether the proposed rule takes effect or is modified in any way before December 1.

Related Practices

White Collar Crime & Government Investigations
Cybersecurity and Privacy
Technology

Related Industries

Technology