Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

New Warrant Power Amplifies Need For Strong Data Security

By **Allison Grande**

Law360, New York (December 1, 2016, 11:00 PM EST) -- A rule change that allows courts to issue broader warrants for access to electronic communications took effect Thursday amid concerns that the measure will invite law enforcement snooping in the name of pursuing hackers, turning up pressure on companies not to fall prey to the types of cyberattacks that invite prying eyes.

The hotly contested change to Rule 41(b) of the Federal Rules of Criminal Procedure replaces the current rule, which limits warrant requests to the search and seizure of property within the court's own district. The new, broader mandate allows courts to issue warrants for remote access to electronic data outside their jurisdiction if the location of the information has been "concealed through technological means" or when the data is in five or more districts.

According to the U.S. Department of Justice, the rule change — floated in 2014 and approved by the U.S. Supreme Court in April — is necessary to help law enforcement combat the growing scourge of "botnets" and other sophisticated cloaking technologies criminals use to conceal their identities and avoid apprehension. Botnets are networks of private computers that are infected with malicious software and controlled as a group without the owners' knowledge.

But tech companies such as Google Inc. and PayPal Inc. and groups including the American Civil Liberties Union and the Electronic Frontier Foundation have countered that the "dangerously broad" amendment would throw the door open to blatant Fourth Amendment violations by giving the FBI free rein to hack thousands of computers at once, including those that belong to "innocent internet users" who have fallen victim to botnets or other malware attacks.

"On balance, I think the rule change is necessary to help law enforcement keep up with the rapid adoption by criminals to technical barriers to investigations," said Ballard Spahr LLP partner and former federal prosecutor Edward McAndrew. "But how the government uses the rule is something that businesses will have to pay close attention to."

Under the new rule, prosecutors will be able to approach a judge in one district that has a nexus to its investigation and get a warrant to remotely search, copy and seize information from a device involved in the probe, but whose location is unknown and may not even be in that jurisdiction. The rule also allows for a single judge to issue a warrant to remotely search and copy information from suspected devices spread across five or more districts, which is usually the case when malware infects unsuspecting computers to form a botnet.

While it still remains to be seen how aggressively or frequently the government will use this expanded power, attorneys say that the amendment will at the very least make the already growing use of cyber warrants continue to climb and further open businesses up to government intrusion into their networks.

“All clients have to be considering the implications of the government being in a position to intrude upon networks, whether they’re networks that have been victimized or a server that is involved in some criminal activity,” said Alston & Bird LLP partner and former federal prosecutor Michael Zweiback. “Criminals sometimes carve out a portion of corporate networks to do their illegal bidding, and the corporation’s IT staff is going to have to be extra vigilant to understand the government may be knocking at its network door.”

While some businesses may welcome the news that the FBI is monitoring or has infiltrated their networks to rid them of malware or other unlawful activity, the new expansion of law enforcement power thrusts to the forefront a concern that has always lingered: the potential for government overreach.

“What will need to be watched [is] whether we see a cyber equivalent of pretext searching, where the government gets a remote access search warrant premised upon probable cause for one type of crime, such as hacking, and in reviewing the data remotely uncovers evidence of another crime,” McAndrew said. “That could potentially be a very big issue and a legitimate concern for businesses that have wide-ranging activities that fall under the scrutiny of law enforcement agents or regulators or could subject them to civil liability.”

This heightened risk that the government will search machines compromised by botnets or otherwise hijacked by criminals gives companies yet another reason to invest heavily in their data security, so that officials don’t look at their networks in the first place.

“At some level, that part of the amendment is less likely to impact businesses that have reasonable security practices and don’t have computers and devices that have been taken over by botnets,” said Mayer Brown LLP partner and former federal prosecutor Marcus Christian.

Attorneys noted that smaller businesses and companies that don’t have the resources or have chosen not to invest in cybersecurity are the most likely to be swept up by criminal activity that could draw in the feds.

“The one thing that we know about the bad guys is they’re going for the lowest-hanging fruit when they hijack computers, and people that are less equipped to protect their computers are most likely to be subject to hijack,” said Dorsey & Whitney LLP partner Robert Cattanach. “And it’s always a possibility that part of the price we pay for living in a highly connected society is that law enforcement will eventually stumble across illegal activity by computer owners when looking into a third party. So companies should in addition be careful what they put on their computers.”

However, the former federal prosecutors who spoke with Law360 were quick to try to temper fears of sweeping Fourth Amendment violations, noting that a magistrate judge will still have to sign off on any search warrant made possible by the amendment.

“The amendment doesn’t change the way that the process already works and the requirements of the Fourth Amendment,” said Erik Rasmussen, cyber practice leader for Kroll’s cybersecurity and investigations practice and a former Secret Service agent. “This amendment doesn’t really impact the

fact that judges can still shoot down or reject these types of warrant."

And attorneys expect that judges won't hesitate to closely scrutinize warrant applications that stem from the rule change, especially considering the complex technical questions that are likely to underpin how agents intend to target suspect computers and attack infected networks.

"Judges have a great deal of discretion, and just because they're allowed to issue a warrant in a particular circumstance doesn't mean that they will," Christian said. "And in some instances, judges can be even more careful when it comes to computer and cybersecurity issues that they may find to be inaccessible in terms of their understanding of technology."

McAndrew predicted that judges would have a host of questions in these types of circumstances about the way the search is going to be carried out, the scope of the search, how the information will be gathered, what will happen to extraneous information, and how long this data will be retained.

"The magistrate judge is the ultimate gatekeeper, and even though the rule allows what the prosecutors are asking for, it's still a question of whether a particular type of search that the government seeks to conduct is reasonable under the circumstances," he said.

The rule change will also almost certainly be subjected to challenges in court by both criminals who have had the power used against them as well as third parties whose computers have been swept up by these searches, attorneys say.

Additionally, although Congress missed its deadline to block implementation of the rule change by passing one of several measures designed to either kill it or delay its start date, lawmakers may still be able to act, especially if constituents, privacy groups or companies continue to press them on the topic as the impact of the amendment becomes apparent.

"Just because Congress failed to delay the passage of the amendment of the rule, that doesn't mean the ship has completely sailed," Christian said. "Although the likelihood of legislation now is less, that doesn't mean it's impossible."

Congress can also force the DOJ to provide it with regular statistics about how the Rule 41 change is being used, Cattanach said.

However, attorneys conceded that it's too early to tell whether concerns about the effect the amendment may have on targets' Fourth Amendment rights will pan out, and will likely come into clearer focus in the months and years to come.

"Like most other rule changes, the devil here — if there is one — is in the rule's application," Jones Day of counsel Jay Johnson said. "Whether the government will, or is even able to, use the new rule in a manner that offends constitution[al] protections remains to be seen and will be watched by advocates on both sides of the debate."

--Editing by Mark Lebetkin and Brian Baresch.