Written by **Michael Tennant** on February 21, 2015

Google Sounds Alarm Over FBI's Proposal for Expanded Hacking Power

Calling the Federal Bureau of Investigation's proposal to expand its authority to hack criminal suspects' computers a "monumental" concern, technology giant Google Inc. is urging an advisory committee to "reject" the proposal.

The FBI is seeking to amend Rule 41 of the rules of federal criminal procedure, which authorizes judges to approve search warrants only when the location of the search is within their judicial district. Arguing that the nature of modern computer networks and the ability to disguise a computer's geographical location have made this requirement untenable, the agency wants the Judicial Conference Advisory Committee on Criminal Rules, a federal court panel, to change the rule to allow judges to issue warrants for searches of computers regardless of their location — even in foreign countries — if the location of "the media or information" sought "has been concealed through technological means."

That may seem like a relatively benign and even necessary modernization of Rule 41. Indeed, the Justice Department has claimed that it is merely seeking to update the rule for the Internet age.

"The proposal would not authorize the government to undertake any search or seizure or use any remote search technique not already permitted under current law," Deputy Assistant Attorney General David Bitkower asserted in a December response to critics. Those critics, he said, "appear to be misreading the text of the proposal or misunderstanding current law."

Google obviously was not convinced. In public comments filed just before the February 17 deadline, Richard Salgado, the company's director of law enforcement and information security, stated, "The proposed amendment substantively expands the government's current authority under Rule 41 and raises a number of monumental and highly complex constitutional, legal, and geopolitical concerns."

"Although the proposed amendment disclaims association with any constitutional questions," Salgado penned, "it invariably expands the scope of law enforcement searches, weakens the Fourth Amendment's particularity and notice requirements, opens the door to potentially unreasonable searches and seizures, and expands the practice of covert entry warrants."

The amendment's vague wording is the primary source of these concerns. "It is unclear what types of searches are being authorized by the proposed amendment," noted Salgado, adding that while "the

proposed amendment provides that the government may use 'remote access' to search and seize or copy electronically stored data," "the term 'remote access' is not defined." However, the sample search warrants submitted to the committee by the Justice Department indicate that among the types of "remote access" the FBI would like to employ is something called Network Investigative Techniques (NIT).

Ahmed Ghappour, a computer-law professor at the University of California's Hastings College of Law and a former computer engineer, explained how NIT works in a September *Just Security* piece:

> Broadly, the term "Network Investigative Techniques," (NIT) describes a method of surveillance that entails "hacking," or the remote access of a computer to install malicious software without the knowledge or permission of the owner/operator. Once installed, malware controls the target computer.
>
> The right Network Investigative Technique can cause a computer to perform any task the computer is capable of — covertly upload files, photographs and stored e-mails to an FBI controlled server, use a computer's camera or microphone to gather images and sound at any time the FBI chooses, or even take over computers which associate with the target (e.g. by accessing a website hosted on a server the FBI secretly controls and has programmed to infect any computer that accesses it).

The sample warrants provide no details with regard to the NIT being deployed or any safeguards in them to protect innocent parties, observed Salgado. "In short," he declared, "'remote access' seems to authorize government hacking of any facility wherever located."

Another thing left unclear in the amendment is "what, precisely, may be searched once the media or information is accessed," wrote Salgado. Nothing in the amendment specifies what is meant by data "concealed through technological means," he asserted, "and, as written can be used to justify searches of widespread and legitimate Internet use," such as Virtual Private Networks (VPN) used by businesses to allow remote access to their networks while obscuring the user's actual location. "Moreover," he pointed out, "the proposed amendment contains no 'intent' element to the concealment, which would require probable cause to believe that the target was purposefully concealing its location." And the amendment does not define what "media" is, which "opens the door to law enforcement's unfettered access to whatever information is accessible on the device being searched — whether that information is stored locally, on a network drive, or in the cloud."

Also, under the proposed amendment, FBI agents could search computers in different locations simultaneously, which would enable them to investigate robot networks, or botnets, malware programs that infect vulnerable computers on networks. "According to the FBI," Salgado noted, "a network of botnets can number 'in the hundreds of thousands or even millions,'" so a warrant giving agents the authority to investigate a botnet could thereby grant them access to millions of computers at once. Furthermore, the amendment allows remote searches whenever "the media are protected computers that have been damaged without authorization." If "damage" includes such things as viruses and malware, argued Salgado, this raises the possibility that agents could search a sizable portion of the computers in the United States, nearly thirty percent of which are estimated to have some form of malware.

All of this leads to Fourth Amendment concerns. To be valid under the Fourth Amendment, search warrants must specify the location of the search and what will be seized. The vagueness of the proposed Rule 41 amendment and the sample warrants suggests that warrants granted under the amended rule

will be rather open-ended, not specifying the particular devices or media to be searched or seized. Even if a warrant is specific, guaranteeing that only the specified media is accessed will be difficult. In addition, the proposed rule allows agents merely to "make reasonable efforts" to serve the warrant on the owner of the searched property or seized information, which Salgado maintained "clearly indicates that warrants … will in many instances be targeted at those to whom no notice can feasibly be given" — a violation of longstanding constitutional jurisprudence.

Then there is the matter of international relations. Since the locations of computers being searched remotely may not even be known at the outset, critics say it is virtually certain that some of the searches will take place in foreign countries, violating international law. The Justice Department has responded to such allegations with the usual "trust us" boilerplate, insisting that the amendment "does not purport" to authorize such searches. But, observed Salgado, "the nature of today's technology is such that warrants issued under the proposed amendment will in many cases end up authorizing the government to conduct searches outside the United States."

Ghappour agrees, calling the proposed amendment "the broadest expansion of extraterritorial surveillance power since the FBI's inception." If enacted, he claimed, the amendment "will result in significant departures from the FBI's customary practice abroad: overseas cyber operations will be unilateral and invasive; they will not be limited to matters of national security; nor will they be executed with the consent of the host country, or any meaningful coordination with the Department of State or other relevant agency" — all of which guarantees conflict with foreign countries, which might well prosecute American agents violating their sovereignty.

Such a significant change in policy clearly should not be enacted in a relatively quiet fashion by unelected officials. As Salgado put it, "Legislation, not rule-making, is the proper way to balance legitimate law enforcement needs with serious constitutional and policy considerations," which is why Google is asking the committee to "leave the expansion of the government's investigative and technological tools, if any are necessary, to Congress."

Whether that will happen remains to be seen. The panel is expected to render a decision on the new Rule 41 in the next few months, but after that, either the Supreme Court or Congress could overturn it. In the meantime, "the right of the people" — whether Americans or foreigners — "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" hangs in the balance.