U.S. Supreme Court Adopts New Rules Affecting Foreign Companies on Warrants, Searches, and Seizures

Adrienne E. Fowler & Yuxi Tian*

The U.S. Supreme Court recently approved changes to the Federal Rules of Criminal Procedure that are likely to broaden the reach of the U.S. government for searching information located outside U.S. borders. The critical amendments apply to Rule 4 and Rule 41. Congress now has an opportunity to reject the amendments. If Congress does not act—and it is unlikely that Congress will—the rules will go into effect in December of this year.

Rule 4 Amendments. These amendments, which apply to arrest warrants and summons on a complaint, extend the U.S. government's authority over foreign companies in a criminal proceeding in several ways. First, an amendment to Rule 4 permits the U.S. government to serve a summons "at a place not within a judicial district of the United States," expressly authorizing the U.S. government to serve a summons outside U.S. borders. The U.S. government may do so by delivering a copy of the summons according to the foreign jurisdiction's law, to any agent legally authorized to receive service of process, or "by any other means that gives notice." Second, Rule 4 would now authorize a judge to take "any action authorized by U.S. law" if an organizational defendant fails to appear in response to a summons. Previously, a foreign defendant had no duty to come to the United States in response to a summons. The amendment now authorizes the court to act, and potentially to impose sanctions, in the event a foreign company defendant chooses to ignore the summons.

Rule 41 Amendments. These amendments are far more controversial. The changes would allow a U.S. judge in any district "where activities related to a crime may have occurred" to issue a warrant to use remote access to search electronic storage media (computers, servers, etc.) and to seize that information, even if that information is located outside the district if:

- "[T]he district where the media or information is located has been concealed through technological means;" or

- The officer seeking a warrant is investigating a botnet or botnets (where a criminal uses malware to unlawfully access or damage a victim's computer or other electronic storage media) involving media located in five or more districts.

The first change does not expressly give U.S. judges the power to authorize the search of a computer or other electronic media outside the United States. But as a practical matter, that will be the result. U.S. courts have interpreted the Fourth Amendment (which limits governmental power to conduct searches and seizures, and which Rule 41 is designed, in part, to effectuate) to apply differently to searches and seizures of property that occur within the United States, and those that occur outside the United States. Inside the United States, authorities generally need a warrant before conducting a search. To conduct a search outside of the United States, the Fourth Amendment generally only requires U.S. authorities to have a reasonable basis for conducting a search; no warrant is required.

The laws of other countries also limit the extent to which U.S. authorities can conduct a search and seizure in another country, so the Department of Justice ("DOJ") generally coordinates with foreign authorities before conducting a search of a computer located outside of the United States. Under the proposed rules, however, where the location of a computer is unknown, the DOJ could get a warrant to search a computer located outside of the United States (as long as the DOJ is unaware it is located outside of the United States), and search it without coordinating with local officials in that other country and without setting foot in the other country. The DOJ has announced that if it learns that it has searched a computer outside of the United States, it will use the existence of a warrant as proof that it had a reasonable basis for the search, which would allow the evidence to be used in a criminal prosecution occurring in the United States.

The second change would allow the authorities to obtain a single warrant to search any number (hundreds, or even thousands) of computers belonging to the victims, rather than the perpetrators of, an illegal botnet. It does not distinguish between personal computers that are infected with malware and computers or servers belonging to a company. There is a possibility that if the search and seizure shows that the botnet victim is him or herself engaging in a crime—and evidence of that crime was in the officer's plain view when investigating the botnet—the evidence could then be used in the prosecution of that second crime. The case law about what is "in plain view" during a computer search varies in different U.S. jurisdictions.

In terms of notice when a warrant authorizes remote access, the officer merely needs to "make reasonable efforts" to serve a copy of the warrant and receipt on the person whose property will be searched. Service can be by electronic means, as long as they are "reasonably calculated to reach that person."

* * *

For more information regarding these updated rules or Harris, Wiltshire & Grannis LLP's international telecommunications, national security, or data protection practices, please contact **Tricia Paoletta** at +1 202 730 1314 or by e-mail at tpaoletta@hwglaw.com, or **Kent Bressie** at +1 202 730 1337 or by e-mail at kbressie@hwglaw.com. Alternatively, you should contact the HWG lawyer with whom you regularly work.

This regulatory advisory is not intended to convey legal advice. It is circulated to HWG clients and friends as a convenience and is not intended to reflect or create an attorney-client relationship as to its subject matter.

*Admitted only in New York. Supervised by Jonathan Mirsky, a member of the DC bar, while DC bar application is pending.