e-commercelawreports

THE PRACTITIONERS' GUIDE TO E-COMMERCE CASES
VOLUME 13 ISSUE 03 **WWW.E-COMLAW.COM**
[2013] ECLR 1 - 24

VOLUME 13 ISSUE 03 **[2013] ECLR 1-24**

FBI warrant to search a target computer at premises unknown

In May 2013, a United States magistrate judge of the United States District Court for the Southern District of Texas denied a request from the FBI to obtain a search warrant to hack an unknown computer in an unknown location to determine who was responsible for crimes committed using the computer.

Background

The FBI's warrant request arose from an incident involving a personal email address of a Texas resident that was hacked in order to access the person's local bank account. The computer that hacked the account had an Internet Protocol (IP) address that resolved to a country in Southeast Asia. After discovering that he was hacked, the Texas resident attempted to secure his email account to prevent further breaches. The hacker then set up a nearly identical email address and used it to attempt to transfer a large sum of money from the Texas resident's local bank to a foreign bank account. The FBI then began an investigation and sought a warrant to identify the target computer and suspects involved in the crimes.

The FBI's warrant application asked for permission to install data extraction software on the target computer, which has the capacity to perform several functions, including the following: search the hard drive, random access memory, and storage media; initiate the computer's built-in camera; identify latitude and longitude coordinates for the computer's location; and send the extracted data to FBI agents in Texas. Generally, the FBI wanted to obtain records that existed on the target computer, including IP addresses, records of internet activity, and evidence of who used the computer and when. The FBI also wanted to monitor the computer for 30 days to obtain data such as accounting entries that could identify new victims of fraud, photographs using the built-in camera to identify users of the target computer, and information about the computer's location. The government asked for the warrant application to be sealed to avoid harming the ongoing investigation. The judge sealed the warrant application, but did not seal the opinion because it relates to a general question of law.

The Court's analysis

The judge noted that the FBI's novel search warrant request hinged on three main questions, namely, whether the FBI's warrant satisfied the following: (1) the territorial limits of a Rule 41 search warrant; (2) the particularity requirements of the Fourth Amendment; and (3) the video surveillance requirements of the Fourth Amendment. The judge discussed each question in turn and concluded that the FBI had not demonstrated the applicable requirements, which led him to deny the FBI's request for a warrant.

Territorial limits of Rule 41

Rule 41 of the Federal Rules of Criminal Procedure identifies five territorial limits on a magistrate judge's authority to issue a warrant. The government invoked only the first subsection of Rule 41, which provides that a judge can only authorise a warrant to search property within the judge's district. The government argued that the FBI warrant meets this requirement because information obtained from the target computer would be reviewed by FBI agents within the magistrate's district in Texas. The judge disagreed, and noted that because intangible computer data can be analogised to a container filled with information, by the government's logic the FBI could 'roam the world' to search for containers of contraband and that would be acceptable as long as the containers were opened in the district issuing the warrant. Also, the judge explained that the FBI actually sought to conduct two searches: (1) an initial search to identify the target computer, and (2) a search of the information on the target computer for criminal evidence. Because the FBI did not know where the target computer was located, the location of the information on the computer was also unknown and the search of that information could potentially occur outside the judge's district. Therefore, the judge concluded that the warrant application could not satisfy the territorial limit of Rule 41 that requires a warrant to be issued within the magistrate's district. Similarly, the judge explained that the warrant does not meet any of the other four territorial limits that the FBI did not address in its application.

Particularity requirements of the Fourth Amendment

The Fourth Amendment states that search warrants must 'particularly describ[e] the place to be searched, and the persons or things to be seized.' The judge explained that the FBI's warrant application did not specify how the agency would find the target computer, which forced the judge to speculate how the FBI would accomplish that task. The judge noted that it could be difficult to identify the target because hackers have ways of disguising their illegal computer activity and using seemingly innocent computers to carry out crimes. Also, the government did not explain how it would avoid placing the proposed intrusive software on innocent computers, or how it would ensure that only those engaging in illegal activity would be exposed to the hacking software. The application did not provide enough information about how the government would accommodate various circumstances that could affect the target computer, for example, if it was a public computer in a library or internet café, or if family or friends not involved in the illegal

activity used the computer. The judge concluded that the limited information in the FBI's warrant application did not satisfy the particularity requirement of the Fourth Amendment.

Video surveillance requirements of the Fourth Amendment

As previously mentioned, the software the FBI proposed in the search warrant would be able to activate the target computer's built-in camera and take pictures of anyone who used the computer. Although the government described the use of the camera as 'photo monitoring' rather than video surveillance, the judge was not convinced. The software would allow the government to have access to the camera in real time and that is equivalent to video surveillance. The judge explained that video surveillance has been deemed the most intrusive method of surveillance by the Fifth Circuit and the court has borrowed from wiretapping statutes to identify constitutional standards for video surveillance. A search warrant for video surveillance must include: (1) a statement that other investigative methods have been tried and failed, or appear too dangerous or unlikely to succeed if tried; (2) a description of the communication the government wants to intercept and what offence the communication relates to; (3) the duration of the surveillance (generally no longer than 30 days); and (4) a statement of steps taken to ensure that surveillance is only used for the intended purpose. US v. Cuevas-Sanchez, 821 F.2d 248, 252 (5th Cir. 1987). The judge concluded that the government's application failed to meet the criteria demonstrating inadequate alternatives and minimisation of intercepting video for the intended purpose. The government offered only conclusory statements for these criteria but did not explain why other methods would not work or how the FBI intended to minimise collecting data only for the purposes for which the FBI requested the search warrant.

The Court's conclusion

The judge found that based on his analysis of the FBI's application to obtain a warrant, the search warrant did not meet the requirements of Rule 41 and the Fourth Amendment. The judge acknowledged that Rule 41 does not necessarily preclude the use of the FBI's requested hacking techniques under any circumstances, and implied that innovations in computer searching technology could warrant changes to the territorial limits of the rule. However, an intrusive search of this nature must meet the requirements of Rule 41 and the Fourth Amendment, and the FBI did not meet its burden here.

Commentary

The lesson from this judge's ruling is that courts may be reluctant to allow the government to obtain overly broad search warrants to investigate cyber attacks carried out using unknown computers in unknown places. The FBI's warrant request amounted to a general warrant of the sort that led to the adoption of the Fourth Amendment, which protects against 'unreasonable searches and seizures.' In this court's view, the government did not satisfy its burden of demonstrating that the warrant met the constitutional standards of the Fourth Amendment such that the FBI could capture data as wide ranging as IP addresses, chat history, browser cookies, and photographs of everyone who used the target computer. Here, the FBI had the added hurdle that the agency did not even know which computer needed to be searched, or where the computer was located.

The computer crimes the FBI sought to investigate raise the ever-present challenge for cyber attacks of determining attribution, which means identifying the actual perpetrator responsible for the cyber attacks. Attribution can be difficult to determine because the computer from which an attack seems to have originated might not be the actual source due to hackers' ability to take over computers and disguise their actions. Therefore, even if the FBI had identified a particular computer to hack, they might not be able to determine with certainty whether the computer was used knowingly and who controlled the computer when it was used to commit the crimes at issue.

Attribution would likely pose a problem for any similar warrants the government may request in the future to hack computers. However, a court may be inclined to authorise such a warrant if the government can overcome the deficiencies in the warrant that the FBI sought in Texas. Specifically, if the warrant application includes more details about the target computer, such as where it is located or even how the target computer will be identified, then a judge might be more likely to authorise the warrant. Additionally, further advances in technology that allow the FBI to pinpoint the target computer may lessen the concern of overreaching and the potential hacking of innocent computers and individuals.

Andrew B. Serwin Partner
Aramide O. Fields Associate
Morrison & Foerster LLP
ASerwin@mofo.com
AFields@mofo.com