BARNES & THORNBURG LLP

Did The Supreme Court Pave The Way For Court-Sanctioned Mass Hacking?

July 19, 2016 | | Case To Watch,The GEE Blog

Meena T. Sinfelt
Partner
White Collar, Compliance and Investigations Co-Chair

In late April of this year, the U.S. Supreme Court adopted an amendment to Federal Rule of Criminal Procedure 41(b) that would allow judges to issue warrants permitting the FBI to access computers located outside the court's jurisdiction. As many technology and privacy groups point out, this proposed change could have a remarkable effect on a judge's ability to issue warrants, not to mention the severe impact on data privacy rights.

Deadline Looms for Congress to Act

Currently, Rule 41(b) only allows a court to issue search and seizure warrants for property located within the issuing court's district. As proposed, the amendment would allow courts to issue warrants authorizing the FBI to remotely access and seize electronic media stored *outside* its district if: a) the true location of the data being sought by the FBI has been hidden or concealed by technology or b) in an investigation of fraud against a financial institution (18 U.S.C. § 1030), the computers have been intentionally damaged and are located in five or more districts. Congress has until Dec. 1, 2016, to act on the proposed amendment. If lawmakers take no action on the proposed amendment it will automatically become effective. Both the House and Senate have considered, but not acted on, alternative legislation known as the Stop Mass Hacking Act, to spur Congressional consideration of the rule change. Senator Ron Wyden (D-OR), who co-sponsored the bi-partisan bill stated, "[s]uch a substantive change with an enormous impact on Americans' constitutional rights should be debated by Congress, not maneuvered through an obscure bureaucratic process."

The Challenge of Fighting Sophisticated Cybercrime

The Department of Justice (DOJ) has been advocating for a change to Rule 41(b) since 2013 as a necessary modification to keep pace with the sophisticated cyber-tactics of criminals. This push for a change to Rule 41(b)'s limits is in response to a number of suppression rulings related to the FBI's investigation of a dark net child pornography website. This website used Tor software, which allows a user's identity to remain anonymous by masking the internet protocol (IP) address. In a warrant obtained in the U.S. District Court for the Eastern District of Virginia (EDVA), the FBI in Virginia was allowed to effectuate "searches" of computers located in various states. The FBI deployed anti-Tor malware (or a network investigative technique) that unmasked the IP addresses of the website's users. In some cases, the FBI

RELATED PRACTICE AREAS

Financial and Regulatory Litigation
Government Litigation
Securities and Capital Markets
White Collar and Investigations

RELATED TOPICS

Data Privacy
Federal Rule of Criminal Procedure

also turned on the end-user's computer camera. The warrant allowed the government to search the computers of 215,000 website users, while also unmasking 1,300 IP addresses. More than 100 arrests were made in the U.S., with many more abroad, producing the inevitable guilty pleas. However, within the past few months several courts have criticized the issuance of the warrant, highlighting the significance of the proposed change to Rule 41(b). In *United States v. Alex Levin*, a Massachusetts District Court granted a motion to suppress evidence on the basis that the EDVA warrant "was issued without jurisdiction and thus" void at its issuance. The court further stated that the resulting search was warrantless, presumptively unreasonable, and that the good-faith exception was inapplicable. This same reasoning was followed by a U.S. District Court in Oklahoma, in *United States v. Scott Fredrick Arterbury*, with the same result of suppression of evidence. However, the U.S. District Court for the Eastern District of Pennsylvania, in *United States v. Werdene,* denied a suppression motion based on the EDVA warrant finding a procedural violation by the issuing magistrate and that the FBI executed the warrant in good faith. Since the network investigative technique surreptitiously places code on a target's computer upon accessing a particular website, it not only gives the government access to the contents of the target's home computer, but also to computers of non-threatening citizens who likewise access the website. If the amendment is approved, a warrant would then allow the government to deploy malware on hundreds of computers connected to any commercial website that is arguably connected to criminal activity, despite the legitimacy of the website itself, for instance, a bank's website. If a user of that commercial website is masking his or her IP identity simply for anonymity, but not for illegal purposes, the user would still be treated in the same way as an illegal hacker. The user's computer could be breached, searched and infected with malware without his or her knowledge and without any particularized probable cause. Once the computer's content is copied, there is little to no oversight in the retention of the information obtained. The government struggles to keep up with the sophisticated, always evolving world of cybercrime. Nevertheless, the government has various means to subpoena information from ISPs without notice to the ultimate user, such as the Stored Communications Act. So the question remains, does the proposed amendment to Rule 41(b) provide a reasonable expansion for government investigations, or is the amendment an invitation for the FBI to search thousands of users' computers for whom they have no indication of criminal activity, thereby compromising the user's Constitutional protection against an unreasonable search? See our subsequent post: Second Circuit Confirms Privacy Rights and Territorial Limits of Search Warrants Under the Stored Communications Act for how this is playing out.