ADDITIONAL CONSIDERATIONS REGARDING THE PROPOSED AMENDMENTS TO THE FEDERAL RULES OF CRIMINAL PROCEDURE

November 28, 2016

Courtesy of Assistant Attorney General Leslie R. Caldwell of the Criminal Division

This blog post addresses several arguments raised by commentators against proposed amendments to the venue provisions of Rule 41 of the Federal Rules of Criminal Procedure. Prior posts addressed the need for an amendment to identify a single court that can hear an application for a search warrant to investigate a nationwide botnet and the need for a related amendment to ensure that investigators can identify at least one court authorized to consider a search warrant application when a criminal has used anonymizing technology.

In two prior posts, I have discussed the dizzying rise of two forms of modern crime: crime committed over the Internet by anonymous users, such as pedophiles who use the Tor network to propagate and encourage the creation of depictions of child sexual abuse; and botnets, or networks of illegally hacked computers that siphon wealth and invade privacy on a massive scale. I have also discussed two straightforward amendments to the venue provisions of the Federal Rules of Criminal Procedure that would clearly identify which court was authorized to consider an application for a search warrant to investigate such crimes. Those amendments were first proposed almost three years ago, and after long consideration and substantial public debate, they were recently approved by the U.S. Supreme Court and will go into effect on Dec. 1, 2016. In this post, I will address some arguments made by commentators who have opposed the amendments, and explain why those arguments are misconceived.

Initially, however, note that these are not the first comments the department has made on this topic—the amendments resulted from a three-year public deliberative process, and many if not all of the objections made today have been previously made and addressed during that process in a series of public hearings and memorandums. Nor will they be the last comments on the topic. If the rules are permitted to go into effect, they will have no different standing than any of the other rules of criminal procedure: they will be subject to oversight by courts and Congress in their use and application. As with all search warrants, warrants issued pursuant to the amended venue provisions will have to be authorized in the first instance by independent federal courts, and will then be subject to challenge after execution as well—if evidence is used in a later prosecution, for example. Nor do we believe that the investigative steps taken by federal law enforcement in our efforts to counteract modern criminals—whether or not they rely on particular venue provisions in the federal rules of procedure—should escape scrutiny. To the contrary, we embrace the robust debate regarding the reasonable measures available to fight crime in a democratic society. But that debate, of course, is only helpful to the extent it relies on accurate information.

To that end, one argument worth dispelling at the outset is the insinuation that the proposed amendments are illegitimate because they were proposed and considered by an "obscure committee," rather than by Congress and without sufficient transparency. This is false. The proposals were adopted on May 1, 2016, by the Supreme Court of the United States—not typically referred to as an "obscure committee"—after extensive public consideration by the federal judiciary. Moreover, the amendments were proposed to and vetted by the federal judiciary pursuant to the statutory mechanism that Congress itself created for consideration of amendments to the rules of procedure. Nor is there anything atypical about the judiciary, rather than Congress, considering and proposing amendments to the venue provisions regarding search warrants in Rule 41. In fact, the exact same process has been used repeatedly over the years to amend the venue section of the rule.

One advantage of the lengthy and deliberative process led by the federal judiciary is that the process created a lengthy record of the discussions that led to the crafting of the rule, objections made, and the response to those objections. In the case of these proposed rules, the committee members—mostly federal judges from around the country, but also state court judges, academics, and defense attorneys—heard and responded to a number of objections, and explicitly rejected many of them on the basis that "much of the opposition reflected a

misunderstanding of the scope of the proposal. The proposal addresses venue; it does not itself create authority for electronic searches or alter applicable statutory or constitutional requirements."

For example, some have criticized the amendments because they believe the new venue rules would allow investigators to apply for a warrant authorizing the search of multiple computers at the same time. But current law already permits investigators to apply for a warrant to search multiple places, accounts or devices at the same time. So long as the application establishes the legal prerequisites for each search, the law does not govern the number of pieces of paper the agents must bring. And even if the law were different, the proposed venue rules would not change it, because all they do is identify the appropriate court to consider an application, not prejudge whether that application must be granted, modified, or denied.

Others have argued that the amendments are problematic because they permit the search of victim computers—that is, computers infected with malware tied to a botnet. To be clear, the "searches" being contemplated here would, typically, be done only to investigate the extent of the botnet, or to obtain information necessary to liberate victims' computers from the botnet. For example, law enforcement could obtain identifying information from bot computers in order to contact owners and warn them of the infection. Or, law enforcement might engage in an online operation that is designed to disrupt the botnet and restore full control over computers to their legal owners. Both of these techniques, however, could arguably involve conduct that would constitute a search or seizure under the Fourth Amendment. Whether or not agents can search a computer infected with malware is a question of substantive law, rather than venue. Existing substantive law expressly contemplates that it may be appropriate to search property belonging to an innocent crime victim. It would be strange if the law forbade searching the scene of a crime. But, again, this law is beside the point because nothing in the venue amendments would affect that law, because the amendments do nothing more than identify the appropriate court to consider an application.

In this vein, some have imagined that changes to the venue provisions will provide the FBI with new authority to conduct "mass hacking" of victim computers. This too is incorrect—the pending amendments do not authorize the government to undertake any search or seizure or use any remote search technique that is not already permitted under the Fourth Amendment. The part of the proposed amendments that deal with anonymized crime have nothing to do with botnet victims. And the only law enforcement actions that would be facilitated by the botnet-focused provisions would be those law enforcement actions that targeted widespread computer hacking by criminals and were expressly approved as consistent with the Fourth Amendment by an independent court. Stated another way, the Constitution already forbids mass, indiscriminate rummaging through victims' computers, and it will continue to do so if the venue rule change goes into effect. By contrast, blocking the amendments would make it more difficult for law enforcement to combat mass hacking by actual criminals.

Some have raised concerns that the use of remote search technique by law enforcement—particularly to assist victims of botnets—could unintentionally damage computer systems. As with law enforcement activities in the physical world, law enforcement actions to prevent or redress online crime can never be completely free of the risk of unintended consequences. For this reason, before we conduct online investigations, the Justice Department carefully considers both the public safety needs and the potential risks. In particular, when conducting complex online operations, we strive to work closely with sophisticated computer security researchers both inside and outside the government. As part of operational mission planning, investigators conduct pre-deployment verification and validation of computer tools. Such testing is designed to ensure that tools work as intended and do not create unintended consequences. That kind of careful consideration of any future technical measures will continue, and we welcome continued collaboration with the private sector and cybersecurity experts in the development and use of botnet mitigation techniques.

But the argument that the possibility of unintended harm attributable to law enforcement should foreclose any investigation of anonymized crime, or any search of computers infected by malware, is absurd. The possibility of such harm must be balanced against the very real and ongoing harms perpetrated by criminals—such as hackers who continue to harm the security and invade the privacy of Americans through an ongoing botnet, or pedophiles who openly and brazenly discuss their plans to sexually assault children. And here again, it is worth emphasizing the limited scope of the proposed amendments: venue. The amendments neither endorse particular searches as reasonable, nor do they in any way change the traditional constitutional, statutory, and prudential factors the department relies on to determine whether to seek a warrant. They simply identify the appropriate court to ask. By

contrast, blocking the proposed amendments would result in there being no venue at all, or at least no practical venue, to seek a warrant to investigate. No one familiar with the harm caused by anonymized child sexual abuse, anonymized firearms trafficking or overseas malware can seriously contend that it makes more sense for Americans to fear federal investigators seeking search warrants from independent federal courts.

Finally, opponents of the rule claim that an amendment to the venue provisions would implicitly repeal the constitutional requirement to establish probable cause or particularity, or the statutory framework governing the use of real-time electronic surveillance of the contents of communications. These claims are mistaken as a basic matter of law, as the judges considering the proposals repeatedly explained. The rules do not make any change to those basic principles. As a matter of basic constitutional law, rules amendments could not make any change to the constitutional requirements of probable cause and particularity. Indeed, we have little doubt that, if the current proposal goes into effect on Dec. 1, many of those now claiming that the proposed rules impliedly repeal the Fourth Amendment or the Wiretap Act will join the department in taking the exact opposite position.

If the rules go into effect on Dec. 1, we do not expect a sudden end to public discussion about their wisdom and effectiveness. We look forward to demonstrating to Congress and the public why these venue changes are essential to protecting Americans, and especially American children, from online criminals. We look forward to continued collaboration with the private sector on best practices in the struggle against botnets and other cybercrime. And, as always, we look forward to continued engagement with those who advocate in favor of privacy protections, whether privacy from the government or privacy from mass criminal hackers.

Posted in:
Criminal Division

RELATED BLOG POSTS

There are currently no blog posts matching your search terms.

Updated November 28, 2016