Search Warrants Authorizing Law Enforcement Computer Hacking and Malware – North Carolina Criminal Law

Jeff Welty ⋮ 7-9 minutes ⋮ 7/23/2018

Suppose that law enforcement becomes aware of criminal activity taking place through a website, like the distribution of child pornography or the sale of illegal drugs. Can officers use computer hacking techniques and malware to identify users who accessed the website? Would the officers need a search warrant to do that? What kind of a search warrant? This post tackles those questions.

Playpen. Most of the case law in this area stems from the federal government's investigation of a child pornography website called Playpen. In early 2105, the FBI took the website over. It operated the site for two weeks – a decision that later generated immense controversy – during which time it deployed malware on users' computers. (The government uses the term "Network Investigative Technique (NIT)" rather than malware, but there is no dispute that the government installed uninvited, unwelcome, and undisclosed code on users' computers, exploiting a security vulnerability in their web browsers.) The malware collected users' IP addresses and other information and sent it to the FBI, enabling the FBI to identify and further investigate the users.

The FBI had obtained a federal search warrant authorizing the use of the malware, but users who were identified and prosecuted as a result of the use of the malware challenged the warrant on several grounds, including lack of particularity and lack of territorial jurisdiction. These cases are working their way through the federal courts now. The most common outcome has been for courts to find that even if there was a Fourth Amendment violation, the evidence obtained using the malware need not be suppressed because the officers relied in good faith on an apparently valid warrant, and under federal law there is an exception to the exclusionary rule under those circumstances. *See United States v. McLamb*, 880 F.3d 685 (4th Cir. 2018) ("Three of our sister circuits have analyzed the same NIT warrant at issue in this case. Each has concluded that even if the NIT warrant violates the Fourth Amendment, the *Leon* good faith exception precludes suppression of the evidence. *See United States v. Horton*, 863 F.3d 1041 (8th Cir. 2017); *United States v. Levin*, 874 F.3d 316 (1st Cir. 2017); *United States v. Workman*, 863 F.3d 1313 (10th Cir. 2017). We agree."). Nonetheless, the opinions shed considerable light on how courts view law enforcement use of hacking techniques and malware. Readers interested in learning more about the Playpen case specifically may wish to consult this primer on the investigation by the Electronic Frontier Foundation.

Legal principles. The Playpen cases and others illuminate certain legal principles:

- *Law enforcement may use hacking techniques and malware under certain circumstances.* It is generally unlawful under federal and state law to hack another person's computer. See, g., G.S. 14-454 (unauthorized access); G.S. 14-458 (computer trespass). But that doesn't mean that law enforcement may never do those things, just as the fact that it is generally unlawful to break and enter a person's home does not mean that law enforcement may never do that. The relevant analytic framework is the Fourth

Amendment. Law enforcement hacking of a person's computer will normally constitute a search of that computer, meaning that law enforcement will typically need a warrant to do so. *See United States v. Horton*, 863 F.3d 1041 (8th Cir. 2017) (use of the Playpen NIT "required a warrant" because users have a reasonable expectation of privacy "in the contents of [their] personal computer[s]"). Occasionally, an exception to the warrant requirement may apply. For example, exigent circumstances might justify the warrantless hacking of a computer if there were probable cause that the user was planning an imminent terrorist attack.

- *Drafting a search warrant authorizing the use of hacking techniques and malware requires careful consideration.* Such a warrant will raise several legal issues not present in typical search warrants, including:
    - Whether the issuing official has territorial jurisdiction over the computers on which the malware will be deployed. This was a major issue in the Playpen case, where the version of Fed. R. Crim. P. 41 in effect at the time the warrant issued only allowed a judicial official to authorize a search of "property located within the district," yet the malware was installed on computers across the country and around the world. While that rule has since been amended, S. 15A-243 still limits the territorial scope of search warrants issued by state judicial officials. Because internet-based criminal activity often crosses state lines, federal authorities may be better positioned to investigate this type of offense.
    - Whether the malware will be deployed immediately upon a user logging in to the target website, or whether some further triggering event, such as accessing specific content, will be required. This was not a concern with Playpen, a dark web site dedicated exclusively to child pornography: the act of logging in to the site provided probable cause that the user's computer contained evidence of child pornography. But it would be a serious concern with sites that mix both lawful and unlawful content or that serve as marketplaces for both legal and illegal products. Generally, search warrants that are triggered by a user's actions should satisfy the requirements of anticipatory search warrants. *See* Robert L. Farb, *Arrest, Search, and Investigation in North Carolina* 431 (5th 2016) (discussing anticipatory warrants).
    - What the malware will do. The Playpen malware harvested a limited amount of identifying information from users' computers, but malware that captures a larger amount of information may require additional scrutiny.
    - How many users will be affected. The Fourth Amendment requires that search warrants "particularly" describe the location to be searched. Professor Orin Kerr argues in this blog post that there may be some limit to the number of users that may be investigated before a warrant becomes general rather than particular.

Parting thoughts. Two last comments. One, if I were an officer seeking a warrant of this kind from a state judicial official, I would probably take it to a superior court judge. Search warrants issued by superior court judges are valid throughout the state, while those issued by district court judges and magistrates have a narrower reach. And going to a judge instead of a magistrate guarantees that the judicial official will be a lawyer, which may be helpful given the novel and thorny legal issues presented by warrants of this kind. Two, if you're interested in more reading on hacking and malware, this ACLU publication is a helpful reference. It's entitled *Challenging Government Hacking in Criminal Cases*, and as the name suggests, it is aimed mainly at the defense bar – but I suspect that other audiences would benefit from it as well.

Previous Chapter Next Chapter