

1 **Rule 41. Search and Seizure**

2 * * * * *

3 **(b) Authority to Issue a Warrant.** At the request of a
4 federal law enforcement officer or an attorney for the
5 government:

6 * * * * *

7 (6) a magistrate judge with authority in any district
8 where activities related to a crime may have
9 occurred has authority to issue a warrant to use
10 remote access to search electronic storage media
11 and to seize or copy electronically stored
12 information located within or outside that district
13 if:

14 (A) the district where the media or information
15 is located has been concealed through
16 technological means; or

17 (B) in an investigation of a violation of
18 18 U.S.C. § 1030(a)(5), the media are
19 protected computers that have been
20 damaged without authorization and are
21 located in five or more districts.

22 * * * * *

23 **(f) Executing and Returning the Warrant.**

24 **(1) *Warrant to Search for and Seize a Person or***
25 ***Property.***

26 * * * * *

27 (C) *Receipt.* The officer executing the warrant
28 must give a copy of the warrant and a
29 receipt for the property taken to the person
30 from whom, or from whose premises, the
31 property was taken or leave a copy of the
32 warrant and receipt at the place where the
33 officer took the property. For a warrant to

12 FEDERAL RULES OF CRIMINAL PROCEDURE

34 use remote access to search electronic
35 storage media and seize or copy
36 electronically stored information, the
37 officer must make reasonable efforts to
38 serve a copy of the warrant on the person
39 whose property was searched or whose
40 information was seized or copied. Service
41 may be accomplished by any means,
42 including electronic means, reasonably
43 calculated to reach that person.

44 * * * * *

Committee Note

Subdivision (b)(6). The amendment provides that in two specific circumstances a magistrate judge in a district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and seize or copy electronically stored information even when that media or information is or may be located outside of the district.

First, subparagraph (b)(6)(A) provides authority to issue a warrant to use remote access within or outside that district when the district in which the media or information is located is not known because of the use of technology such as anonymizing software.

Second, (b)(6)(B) allows a warrant to use remote access within or outside the district in an investigation of a violation of 18 U.S.C. § 1030(a)(5) if the media to be searched are protected computers that have been damaged without authorization, and they are located in many districts. Criminal activity under 18 U.S.C. § 1030(a)(5) (such as the creation and control of “botnets”) may target multiple computers in several districts. In investigations of this nature, the amendment would eliminate the burden of attempting to secure multiple warrants in numerous districts, and allow a single judge to oversee the investigation.

As used in this rule, the terms “protected computer” and “damage” have the meaning provided in 18 U.S.C. §1030(e)(2) & (8).

The amendment does not address constitutional questions, such as the specificity of description that the Fourth Amendment may require in a warrant for remotely searching electronic storage media or seizing or copying electronically stored information, leaving the application of this and other constitutional standards to ongoing case law development.

Subdivision (f)(1)(C). The amendment is intended to ensure that reasonable efforts are made to provide notice

14 FEDERAL RULES OF CRIMINAL PROCEDURE

of the search, seizure, or copying to the person whose information was seized or copied or whose property was searched.