



The U.S. Judicial Conference recently received public comments on proposed amendments to [Federal Rule of Criminal Procedure 41](#) (the "Rule"), which would enlarge DOJ's ability to remotely access, search, and seize electronically stored information ("ESI").

Under the current Rule, a magistrate judge's authority to issue warrants is limited to persons or property located within the district where the court sits, with few narrow exceptions. Given the Rule's territorial limit, DOJ has faced barriers in investigating and prosecuting Internet-based crimes where the computer's location was unknown because of anonymizing tools, or where media and ESI were located in multiple districts or in the Cloud. Under the [proposed Rule](#), a magistrate judge would be authorized to issue warrants permitting the government to "use remote access to search electronic storage media and seize or copy electronically stored

information located within or outside" the district where the court sits, in two possible scenarios. One of these scenarios is DOJ investigations under the Computer Fraud and Abuse Act where the media to be searched are computers protected under the statute that are located in five or more districts. The second scenario is where the location of the media or information has been "concealed through technological means." In these scenarios, the proposed Rule would allow the government to obtain warrants authorizing it to hack into computers and access ESI saved virtually anywhere in the United States, including in the Cloud. **"Remote access":** The proposed amendments do not define what types of "remote access" the government may use to access and search media and ESI. The American Civil Liberties Union (the "ACLU") commented that the FBI has regularly used malware to covertly access information stored on a target's computer, and that such malware can obtain not only a computer's IP address but also the user's Internet activity history, saved user names and passwords, email contents, chat messages, and other information. In addition, these malware can remotely enable the GPS chip, microphone, or camera on a mobile device to track the user's location and capture audiovisual information. The ACLU reported that the government is paying to discover vulnerabilities in software that enable installation of these hacking tools. **"Concealed through technological means":** This precondition to obtaining a warrant under the proposed Rule is ambiguous and potentially broad. The Center for Democracy and Technology commented that technologies concealing the location of media and ESI exist today for legitimate reasons. For example, close to half of all U.S. businesses use Virtual Private Network ("VPN") technology to enable users to interact with confidential business information when accessing such information via unencrypted wifi signals in airports and other public places. Apple's iOS mobile operating system lets iPhone users access wifi networks using random, software-generated network interface addresses rather than the unique identifiers burned into their iPhones, to prevent retailers from tracking iPhone users' shopping patterns when moving about in public places. Under the proposed Rule, the use of these and other widely-used technologies could potentially be enough to trigger the precondition to obtaining a warrant. **Constitutional concerns:** The Fourth Amendment provides that no warrant shall issue but upon probable cause and particularly describing the place to be searched and the persons or things to be seized. While the proposed amendments purport not to address constitutional questions, leaving their resolution to the courts, objectors disagreed. Where the identity or location of the media to be searched is unknown, one of the very objectives of the search is to retrieve the media's location and other identifying information. In these situations, the government cannot "particularly describ[e]" the thing to be searched, and is likely to search computers of individuals as to whom it lacks probable cause. To obtain a warrant for real-time surveillance of wire, oral, or electronic communications, the government must satisfy the Wiretap Act's heightened requirements, including showing that normal investigate procedures have failed or are too dangerous or unlikely to succeed. Objectors complain that the proposed amendments could be an end-run around the Wiretap Act's safeguards. Under the theory that Federal Rules of Procedure are limited to regulating procedure and must not abridge, enlarge, or modify any substantive right, objectors have called for Congress, rather than the Judicial Conference, to define the scope of the government's power to access, search, and seize media and ESI. Written comments received at last week's public hearing can be found [here](#). The public comment period ends on February 17, 2015.

Explore more in

[White Collar & Investigations](#)

Blog series

White Collar Briefly

Drawing from breaking news, ever changing government priorities, and significant judicial decisions, this blog from Perkins Coie's White Collar and Investigations group highlights key considerations and offers practical

insights aimed to guide corporate stakeholders and counselors through an evolving regulatory environment.

[View the blog](#)