



Congress Must Pass the Stopping Mass Hacking Act

On May 1, 2015, the Supreme Court transmitted to Congress an amendment to Rule 41 of the Federal Rules of Criminal Procedure, proposed by the Department of Justice and approved by the obscure Advisory Committee on the Federal Rules of Criminal Procedure. Rule 41 governs when federal magistrate judges may issue warrants, and this rule change would drastically expand these powers, and could significantly expand government hacking as a result.

Congress can stop this dangerous rule from going into effect on December 1, 2016, by passing the [Stopping Mass Hacking Act](#) (SMH Act; S. 2952; H.R. 5321).

- **Rule 41 Amendment would expand the government's hacking activities in two ways:**
 - Remove Jurisdictional Requirements: Except for in limited circumstances, judges may only issue a warrant for a search within their jurisdiction. The Rule 41 change would undermine that jurisdictional requirement and let the government go to any federal magistrate judge where "activities related to a crime may have occurred" -- essentially anywhere in the country -- to get a warrant to remotely hack computers, even when it doesn't know their location.
 - Allow Hacking of Innocent Americans: It would allow that government to hack into innocent people's computers based on the fact that they have already been the victims of computer crime, such as computers that - unknown to their victims - have been turned into part of a botnet. This means that one warrant from one judge could potentially lead to the government hacking thousands or even millions of innocents' computers.
- **Rule 41 Amendment constitutes executive overreach:**
 - What the Advisory Committee on Rules of Criminal Procedure does: The Advisory Committee is only authorized to issue procedural rules. However, the amendment would make substantive law. Therefore, by going to the Advisory Committee - an arm of the judiciary - to obtain this rule change instead of seeking legislation from Congress, the Justice Department usurped Congress' authority to make law and engaged in executive overreach.
 - Why the Rule 41 Amendment is substantive and not procedural: The Rule 41 change is substantive because it presumes that hacking is already lawful, despite that fact that Congress has never legislated on whether the government should hack, let alone established necessary rules or protections as it did with wiretap orders. Additionally, the impact of the rule - the vast expansion of government hacking - is itself highly substantive because of the significant impact it would have on Americans' privacy and cybersecurity.

- **Rule 41 Amendment raises serious constitutional and cybersecurity concerns:**
 - Harming Innocent Victims of Computer Crime or Third Parties: When the government hacks into a computer that has become part of a botnet in order to “clean” the computer - a term that has not been clearly defined - it could unintentionally destroy data on the computer crime victim’s network or device, or otherwise harm the device. Additionally, when the government uses malware, it risks the malicious code spreading to non-targeted networks and devices. Finally, if the government uses a zero-day exploit to hack into targeted devices or networks, but does not disclose that exploit to the developer or the product or service, it prolongs the risk that innocent Internet users will be hacked by malicious third parties who discover that exploit.
 - Fourth Amendment Concerns: Telephone calls used to be the primary means by which Americans communicated some of the most private details of their lives. Today, we share and store that and far more personal information on the Internet and on connected devices. Government hacking can reveal detailed information not only including communications contents, but also personal information such as political and religious leanings, financial and medical information, reading interests and hobbies, location information, and much more, and as such, the practice is far more invasive of Americans’ privacy than wiretaps. However, where wiretaps are subject to strict rules and privacy protections set forth by Congress, the FBI has been using hacking as an investigative technique for well over a decade, even though Congress has never considered whether it is appropriate, let alone what the rules of the road should be to ensure that the FBI and Department of Justice’s investigate technique comply with Fourth Amendment privacy protections.
 - Abuse by Forum Shopping: Without the protections of current jurisdictional requirements, the government could engage in a troubling practice called “forum shopping,” where it purposefully applies for warrants from certain magistrate judges that it believes are most likely to issue a favorable decision, even when those judges would have been unlikely to have jurisdiction, if not for this rule change.
- **What Must Be Done:** Congress should rein in this act of executive overreach and stop the Rule 41 Amendment from going into effect on December 1 by passing the SMH Act. Whether the government should hack, and if so, what the rules of the road should be, deserves rigorous public debate. It should not be decided by obscure bureaucratic bodies like the Advisory Committee.
- **Why Congress Must Act Now:** Government hacking policies significantly impact the cybersecurity and privacy of all Americans. Though little information has been made public, it appears the FBI has been hacking for over a [decade](#), despite never having sought or received approval from Congress. Additionally, federal magistrate judges that approve the government’s requests to hack often [don’t fully understand](#) what it is they are authorizing, and the government uses unexplained phrases like “network investigative techniques” that obscures the fact that the government will be using malware or other common hacking techniques. Given the risks to cybersecurity and privacy, Congress should not wait until after the Rule 41 Amendment has gone into effect and government hacking has significantly expanded to have this necessary public debate. We should have it now.