June 21, 2016

The Honorable Paul Ryan
Speaker
H-232 The Capitol
Washington, DC 20515

The Honorable Nancy Pelosi
Minority Leader
H-204, US Capitol
Washington, DC 20515

The Honorable Mitch McConnell
Majority Leader
317 Russell Senate Office Building
Washington, DC 20510

The Honorable Harry Reid
Minority Leader
522 Hart Senate Office Building
Washington, DC 20510

Dear Speaker Ryan, Leader Pelosi, Leader McConnell, and Leader Reid:

We write to oppose the proposed changes to Rule 41 of the Federal Rules of Criminal Procedure. As technology companies and public interest groups committed to a secure and privacy-protective Internet, we understand that the changes would threaten the civil liberties of everyday Internet users. Absent legislation, the changes will go into effect automatically on December 1. We therefore urge you to reject the proposed updates and to support the Stopping Mass Hacking Act (S. 2952, H.R. 5321), bipartisan legislation that would block the changes. This will give Congress the opportunity to consider and debate the important policy implications of the new powers contemplated by the proposed rule.

The changes to Rule 41 give federal magistrate judges across the United States new authority to issue warrants for hacking and surveillance in cases where a computer's location is unknown. This would invite law enforcement to seek warrants authorizing them to hack thousands of computers at once—which it is hard to imagine would not be in direct violation of the Fourth Amendment. It would also take the unprecedented step of allowing a court to issue a warrant to hack into the computers of innocent Internet users who are themselves victims of a botnet. This proposal is dangerously broad. It fails to provide appropriate guidelines for safeguarding privacy and security, and it circumvents the legislative process that would provide Congress and the public the critically necessary opportunity to evaluate these issues.

Security experts have decried the changes to Rule 41, stating that increased government hacking will likely have unintended consequences that cause serious damage to computer security and negatively impact innocent users.

Indeed, Congress has never authorized government hacking as an investigative tool in this manner and has not established clear rules for when and how such dangerous techniques should be used. In order to conduct searches and seizures under the rule change, government agents will exploit security vulnerabilities that impact millions of computer users. Whenever the U.S. government uses

such vulnerabilities instead of working to see them swiftly fixed, other governments and malicious hackers will be able to exploit them as well.

Furthermore, when using hacking techniques, government agents will have access to huge amounts of sensitive information. The rule changes do not impose any additional protections to address the heightened impact that government hacking will have on Internet users' security and privacy.

The rule changes attempt to sidestep the legislative process by using a process designed for procedural rules to expand investigatory powers. Congress and the public need adequate time to have an informed debate about government hacking—and an opportunity to consider what safeguards must be instituted—before the usage of these dangerous investigative tools becomes widespread.

The rule changes exacerbate existing problems; they do not fix them. The amendments would encourage forum shopping for warrants, allowing the government to repeatedly use those magistrates who take the most lax view in reviewing warrant applications to authorize the hacking of users around the world.

Moreover, the changes to Rule 41 will disproportionately undermine the privacy of those who have done the most to protect it. Specifically, the proposal would allow warrants for remote hacking in cases where privacy protective technologies obscure the location of a computer. There are countless reasons people may want to use technology to shield their privacy. From journalists communicating with sources to victims of domestic violence seeking information on legal services, people worldwide depend on privacy tools for privacy, personal safety, and data security. Many businesses even require their employees to use virtual private networks for security, especially during travel. Such tools should be actively promoted as a way to safeguard privacy, not discouraged.

The Stopping Mass Hacking Act offers a simple solution: it rejects the changes to Rule 41. Passing this bill by December 1 will ensure that Congress has time to fully consider the issue of government hacking before this practice becomes widespread. We urge you to support this bill and to reject the changes to Rule 41.

Sincerely,

Access Now
ACI-Participa
Advocacy for Principled Action in Government
American Civil Liberties Union
American Library Association
Amicus
AnchorFree
Australian Privacy Foundation

Brave
Center for Democracy & Technology
Computer & Communications Industry Association (CCIA)
Constitutional Alliance
Data Foundry
Disconnect
DuckDuckGo
Electronic Frontier Foundation
Fight for the Future
Free Press Action Fund
Freedom of the Press Foundation, creators of SecureDrop
Demand Progress
Evernote
Golden Frog
Google
Government Accountability Project
Hide My Ass VPN Service
i2coalition
International Modern Media Institute
Internet Archive
Internet Association
IP Justice
Karisma
La Quadrature du Net
LEAP
National Association of Criminal Defense Lawyers
New America's Open Technology Institute
Niskanen Center
Open Media
Open Net Korea
PayPal
Privacy International
Private Internet Access
R Street Institute
Reform Government Surveillance
Restore the Fourth
Riseup
Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic
SpiderOak
Tor Project
Wickr Foundation
X-Lab