REPORTERS COMMITTEE
FOR FREEDOM OF THE PRESS

1156 15th St. NW, Suite 1250
Washington, D.C. 20005
(202) 795-9300
www.rcfp.org

Bruce D. Brown
Executive Director
bbrown@rcfp.org (202) 795-9301

February 17, 2015

Members of the Advisory Committee on Criminal Rules

Re: Comment of the Reporters Committee for Freedom of the Press on the Proposed Amendment to Federal Rule of Criminal Procedure 41 Concerning "Remote Access" Searches of Electronic Storage Media and Electronic Information

The Reporters Committee for Freedom of the Press ("Reporters Committee") appreciates this opportunity to comment on the proposed amendment to Rule 41 of the Federal Rules of Criminal Procedure concerning "remote access" searches of computers and other electronic devices. The amendment was proposed by the Department of Justice and modified by the Committee in April 2014.[1]

The Reporters Committee is a voluntary, unincorporated association of reporters and editors dedicated to safeguarding the First Amendment rights and freedom of information interests of the news media and the public. The Reporters Committee has provided assistance, guidance, and research in First Amendment and freedom of information litigation since 1970. The Reporters Committee frequently represents the interests of the press and the public before Article III courts. The Reporters Committee is concerned that the proposed amendment to Rule 41 would intrude on vital constitutional and statutory rights protecting the news media and the free press.

If amended as proposed, Rule 41 would permit a court in a district where activities related to a crime have occurred to issue a warrant authorizing remote access searches of electronic storage media and electronic information located within or outside that district.[2] Under the proposed amended Rule 41, magistrates would be able to exercise this power:

i. When the physical location of the media or information is "concealed through technological means," or
ii. In an investigation of 18 U.S.C. 1030(a)(5), when the damaged protected computers are located in five or more districts.[3]

The proposed amendment presents significant legal and policy issues for journalists and their sources. In particular, the Reporters Committee is

[1] *See generally* Advisory Comm. on Criminal Rules, Materials for April 7–8, 2014 Meeting 155–266 ("Advisory Comm. Materials") (April 7-8, 2014), *available at* http://1.usa.gov/1o8ocLf.

[2] *See, e.g., Memo to Members,* Advisory Comm. Materials at 155.

[3] Under 18 U.S.C. § 1030(e), the term "damage" means "any impairment to the integrity or availability of data, a program, a system, or information," and the term "protected computer" means any computer "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States."

concerned about the vague definition of remote access, which could reveal sensitive journalist-source communications; language such as "concealed through technological means," which may lead to the potential targeting of journalists who use anonymization tools in connection with newsgathering, including to protect their communications with sources; and the absence of language that would prevent law enforcement from impersonating the news media when it seeks to carry out remote access searches.

Of particular concern is the inability of law enforcement officials to know, before applying for a warrant under the proposed amendment to Rule 41, whether the computer or electronic storage medium that is the target of a search belongs to a journalist using an anonymization tool in connection with newsgathering. Computers and electronic storage devices such as hard drives, cell phones, and cloud storage are integral to the modern journalistic profession. As the Supreme Court has recognized, digital devices such as cell phones "are capable of storing and accessing a quantity of information, some highly personal, that no person would ever have had on his person in hard-copy form."[4] Searching electronic storage devices for evidence of a crime is akin to simultaneously rifling through a journalist's "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."[5]

Indeed, any search of a journalist's computer or other electronic devices implicates the Privacy Protection Act of 1980 ("PPA"), which prohibits searches and seizures of work product and documentary materials held by a person with "a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication," with a few expressly enumerated, and very narrow, exceptions.[6] Searches of reporters' electronic devices also implicate the First Amendment rights of the press.

Rule 41 may "not modify any statute regulating search or seizure."[7] As a practical matter, however, the proposed amendment to the Rule places journalists' statutory and constitutional rights at risk by sanctioning the remote access of electronic devices to search for evidence of a crime without requiring that any determination be made prior to such a search as to whether the targeted devices are being used for newsgathering. To be in accord with the PPA and the First Amendment, any amendment to Rule 41 that is intended to allow for remote access searches by law enforcement must ensure that such searches will not compromise the work product and communications of journalists who may use anonymization tools in connection with newsgathering, including to protect the identities of and their communications with confidential sources.

As the Committee considers this amendment, it must take into account that the language and vagueness of the proposed Rule creates serious, far-reaching threats to the constitutional, common law, and statutory rights that protect journalists and media in the

[4] *Riley v. California,* 134 S. Ct. 2473, 2490.

[5] *Id.* at 2496–97 (Alito, J., concurring).

[6] 42 U.S.C. § 2000aa.

[7] Fed. R. Crim. P. 41(a).

United States. Indeed, because the proposed amendment to Rule 41 would substantially abridge and modify essential rights under the PPA and the First Amendment, these issues are beyond the scope of the Federal Rules of Procedure, and any potential changes should be addressed by Congress.[8] We urge the Committee to reject the proposed amendment to Rule 41 in full.

I. The proposed amendment to Rule 41 offers insufficient safeguards for newsgathering and other First Amendment-protected activity.

Remote-access searches of journalists' computers can reveal a variety of confidential information, including lists of contacts, work product, and reporter-source communications. While the Constitution, common law, and statute protect against needless searches targeting the news media, the proposed amendment to Rule 41 would allow the government to circumvent those restrictions when it comes to journalists employing anonymization tools to protect their own privacy and that of their sources.

A. The First and Fourth Amendments and the PPA protect journalists against searches of their communications and work product.

The Fourth Amendment prohibition on unreasonable searches of "persons, houses, papers, and effects" arose from a long list of abusive practices in the colonial era, many of which targeted printers and publishers of dissenting publications.[9] As a result, the Fourth Amendment's roots are intertwined with the First Amendment's guarantees of free speech and a free press. Indeed, the history of the Fourth Amendment is "largely a history of conflict between the Crown and the press."[10]

Because of the historic link between the First and Fourth Amendments, the Supreme Court found in *Zurcher v. Stanford Daily* that where materials to be searched or seized "*may be protected by the First Amendment*, the requirements of the Fourth Amendment must be applied with 'scrupulous exactitude.'"[11] The Fourth Amendment case law relied upon in *Stanford Daily* also calls for "consideration of First Amendment values in issuing search warrants."[12] The Government has proposed that the amended Rule "does not address any constitutional questions" regarding whether a given search is constitutional under the Fourth Amendment.[13] However, neither the Government nor the Committee have addressed the difficulty of considering First Amendment values in the context of a remote access search, as *Stanford Daily* makes clear is mandated by the Constitution.

---

[8] *See Sibbach v. Wilson & Co.*, 312 U.S. 1, 10 (1941).

[9] U.S. Const. amend. IV; *see also, e.g.*, *Entick v. Carrington*, 19 How. St. Tr. 1029 (1765) (dismissing a general warrant against a dissenting printer); *Wilkes v. Wood*, 19 How. St. Tr. 1153 (1763) (same).

[10] *Stanford v. Texas*, 379 U.S. 476, 482 (1965).

[11] *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1979) (emphasis added).

[12] *Id.* at 565.

[13] Advisory Comm. Materials at 158.

Remote access searches of journalists' computers and electronic storage media raise statutory questions as well. The proposed amendment to Rule 41 would permit law enforcement to obtain a remote access warrant to search for evidence of crime. With quite limited exceptions, the PPA bars such searches when the documents to be searched for or seized are related to newsgathering.[14] The PPA was enacted in response to *Stanford Daily*, in which the Supreme Court ruled that the Fourth Amendment's requirements of probable cause, particularity, and reasonableness "should afford sufficient protection against the harms that are assertedly threatened by warrants for searching newspaper offices."[15] Congress disagreed that Fourth Amendment safeguards were sufficient to protect First Amendment activity. Recognizing the "threat that *Stanford Daily* poses to the vigorous exercise of First Amendment rights," Congress prohibited searches for "work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication."[16] Congress also barred searches for "documentary materials" possessed for the same purpose.[17]

The PPA "affords the press and certain other persons not suspected of committing a crime with protections not provided currently by the Fourth Amendment."[18] Thus, it protects journalists who may possess evidence of a crime, but who are not themselves suspected of criminal activity. The proposed amendment to Rule 41 contravenes these protections insofar as it would permit "remote access searches" for work product or documentary materials without any investigation into or determination as to whether those materials are possessed in connection with a purpose to publish or communicate.[19] Those searches could reveal the identities of journalists' confidential sources and the contents of sensitive reporter-source communications, among other newsgathering material, and thus interfere with the flow of information to the public.

B. Remote access searches can unmask reporters' confidential sources and communications.

Many significant pieces of American journalism have relied heavily on confidential sources. The *New York Times* used such contacts to break the story that the NSA had an illegal wiretapping program that monitored phone calls and email messages

---

[14] 42 U.S.C. § 2000aa; *see also Guest v. Leis*, 255 F.3d 325, 340 (6th Cir. 2001). The statutory definition of "documentary materials" is "materials upon which information is recorded," and "includes, but is not limited to, written or printed materials, photographs, motion picture films, negatives, video tapes, audio tapes, and other mechanically, magnetically, or electronically recorded cards, tapes, or discs."

[15] *Stanford Daily*, 436 U.S. at 565.

[16] 42 U.S.C. § 2000aa(a).

[17] 42 U.S.C. § 2000aa(b).

[18] S. Rep. No. 96–874, at 4 (1980).

[19] The PPA requires a "reasonable investigation" of an entity before a search in order to ensure that the entity does not possess the sought-after materials in connection with a purpose to distribute a communication to the public. *See, e.g.*, *Steve Jackson Games, Inc. v. Secret Service*, 816 F. Supp. 432, 440–41 (W.D. Tex. 1993) (finding the Secret Service liable for PPA violations in part because it failed to "make a reasonable investigation" of a publisher before it seized the publisher's work product).

involving suspected terrorist operatives without the approval of federal courts.[20] The *Times* also used confidential sources to report on the waterboarding and other so-called "enhanced interrogation techniques" that terrorism suspects in U.S. custody have faced.[21] The *Washington Post* relied on confidential government sources, among others, to break the story of the Central Intelligence Agency's use of "black sites," a network of secret prisons for terrorism suspects.[22] The identities of confidential sources like these could be easily obtained and revealed if law enforcement uses remote access to search a journalist's device.

The proposed amendment to Rule 41 offers no protections for these confidential documents and communications. By broadening federal law enforcement's ability to search journalists' work product, communications, and contacts remotely, without probable cause to suspect them of a crime, the proposed amendment to Rule 41 would significantly chill reporter-source communications, contrary to the public interest in government accountability. As the Supreme Court has recognized, "Awareness that the Government may be watching chills associational and expressive freedoms."[23] In other contexts, journalists have reported that the knowledge of call metadata monitoring has made sources unwilling to speak to them, even on unclassified matters.[24] And elsewhere, the use of remote monitoring of reporters' satellite phones may have put those reporters' lives at risk.[25] If anonymization tools placed reporters at greater risk of being targeted by law enforcement, reporter-source communications would suffer, impeding newsgathering as a result.

Under the proposed amendment to Rule 41, those journalists who are adopting new encryption and anonymization technologies in order to safeguard their sources and materials are at particular risk. Journalists routinely use anonymization tools to safeguard their sources and communications. Encryption helps journalists protect the content of their communications by scrambling the information in a way that only allows intended recipients to read it. Journalists can use encryption to prevent outside parties from reading or listening to a variety of digital communications by encrypting Internet traffic

---

[20] *See, e.g.,* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times (Dec. 16, 2005), *available at* http://nyti.ms/neIMIB.

[21] *See, e.g.*, Scott Shane, David Johnston, James Risen, *Secret U.S. Endorsement of Severe Interrogations*, N.Y. Times (Oct. 4, 2007), *available at* http://nyti.ms/1dkyMgF.

[22] *See, e.g.,* Dana Priest, *CIA Holds Terror Suspects in Secret Prisons*, Wash. Post (Nov. 2, 2005), *available at* http://wapo.st/Ud8UD.

[23] *United States v. Jones*, 132 S.Ct. 945, 956, 565 U.S. __, __ (2012) (slip op., at 3) (Sotomayor, J., concurring).

[24] In a report that former *Washington Post* executive editor Leonard Downie Jr. wrote for the Committee to Protect Journalists, numerous journalists said surveillance programs and leak prosecutions deter sources from speaking to them. Comm. To Protect Journalists, *The Obama Administration and the Press: Leak investigations and surveillance in post-9/11 America* 3, Oct. 10, 2013, http://bit.ly/1c3Cnfg; *see also With Liberty to Monitor All: How Large-Scale Surveillance is Harming Journalism, Law and American Democracy* 25, Human Rights Watch (July 2014), http://bit.ly/1uz3CL1.

[25] *See, e.g.*, Rod Nordland and Alan Cowell, *Two Western Journalists Killed in Syria Shelling*, N.Y. Times (Feb. 22, 2012), *available at* http://nyti.ms/19leEe6 (reporting that journalists killed in Syria may have been targeted by government forces who traced their satellite phones).

and stored data. Sophisticated systems can even mask who is communicating with whom, or that any communication took place at all. Reporters use encryption to protect themselves, their sources, and the newsgathering process. These practices are likely to become increasingly prevalent as journalists become more aware of the threats insecure communications pose to their sources, communications, and work product.

To protect metadata—the data about data, including when and with whom a person is communicating—journalists need to use anonymity tools that hide the location and identity of the sender of a communication. One such tool, Tor, also protects communications and sources from passive Internet surveillance known as "traffic analysis" which can allow an outsider to ascertain who is talking to whom and thereby track interests and behavior.[26] Tor protects journalists from this surveillance by distributing journalists' transactions over several places on the Internet, so no single point can link the journalist to his or her destination.

Indeed, while remote access searches pose serious dangers to the confidentiality of reporter-source communications and to journalists' security, the proposed amendment to Rule 41 includes no protections whatsoever for journalists, reporters, or other non-suspects who are engaged in First Amendment activity. The Reporters Committee urges the Committee to consider these important First Amendment values and reject the proposed amendment to the Rule.

The proposed amendment to Rule 41 would allow a judge to issue a warrant authorizing law enforcement "to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district."[27] The proposed amendment and the proposed committee note do not define "remote access," although Department of Justice submissions to the Subcommittee on Rule 41 provide some explanation.[28]

Remote access searches could reveal the identities of sources and the contents of reporter-source communications in myriad ways. First, remote access searches can reveal a substantial amount of sensitive information on a person's electronic device, including contacts and geo-location information, a computer's MAC address, operating system, registered user of the operating system, and the address of the last website visited in the user's web browser, among other information.[29] This technology can also be used to remotely control communication devices such as webcams and microphones.[30]

The scope or extent of any remote access search involving the installation of malware could also make reporters' communications, contacts, and work product

---

[26] *See, e.g.,* Tor: Overview, https://www.torproject.org/about/overview.html.en.

[27] *See, e.g.,* Proposed Amendments Materials at 338.

[28] *See generally* Advisory Comm. Materials at 179–235.

[29] *See, e.g.,* Kevin Poulson, *FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats*, Wired (July 18, 2007), *available at* http://wrd.cm/1v12K2D

[30] *See e.g.,* Craig Timberg and Ellen Nakashima, *FBI's search for 'Mo,' suspect in bomb threats, highlights use of malware for surveillance*, Wash. Post (Dec 6, 2013), *available at* http://wapo.st/1gdutVf.

susceptible to ongoing vulnerabilities. Since at least the early 2000s, federal law enforcement agencies have used sophisticated surveillance software in national security and criminal investigations to remotely access targeted computers.[31] Yet security flaws have been repeatedly discovered in popular interception and surveillance tools, leading to vulnerabilities that can be exploited by other adversaries.[32] In addition, once malware is released into the "wild" (i.e. where it is able to infect computers) it can be difficult to contain. It can collect information in an ongoing manner and outside the scope of the original purpose.[33] Security flaws such as these can put reporters and their sources at risk.[34]

C. The proposed amendment offers no protection to journalists who use anonymization tools to protect communications with and identities of sources

If the proposed amendment is adopted, a warrant could be issued to remotely search and seize or copy electronic media outside the district when the physical location of the media or information is "concealed through technological means." The Reporters Committee is concerned that this language, if adopted, will affect journalists who use encryption[35] and anonymity tools[36] to improve their own security and privacy and that of their sources.

The use of anonymization tools such as Tor has become a best practice for reporters to safeguard the confidentiality of their work product, communications, and sources. Prestigious journalism schools like Columbia University's Graduate School of Journalism and its Tow Center for Digital Journalism have conducted research into digital security practices for journalists, including how best to systematically integrate

---

[31] *See e.g.,* Reuters, *FBI Sheds Light on 'Magic Lantern' PC Virus*, Reuters, (Dec. 13, 2001) *available at* http://usat.ly/1DCnsYg.

[32] *See, e.g.,* Craig Timberg, *German researchers discover a flaw that could let anyone listen to your cell calls,* Wash. Post (Dec. 18, 2014), *available at* http://wapo.st/1AkQ7zt; *see also* National Security Agency, DOCID No. 352694, Phone Freaks Can Invade Your Privacy (1976), available at http://explodingthephone.com/docs/db904 (declassified NSA memo describing how interfaces used by phone company employees to determine if a line was busy were subverted by outsiders to listen to phone conversations).

[33] *See, e.g.,* Rachel King, *Stuxnet Infected Chevron's IT Network*, Wall St. J. (Nov. 8, 2012), http://blogs.wsj.com/cio/2012/11/08/stuxnet-infected-chevrons-it-network/

[34] See, e.g., Matthieu Aikins, *The spy who came in from the code*, Columbia J. Rev. (May 3, 2012), available at http://bit.ly/1L1BK7j (detailing how lack of digital security protections exposed journalists' Syrian sources to retaliation by intelligence services).

[35] Encryption is a process that involves making a message unreadable except to the person who knows how to decrypt it back into readable form. Encryption can be used across a variety of platforms, including phone, Voice over Internet Protocol (VoIP), email, online chat and file-sharing.

[36] Tools that can help provide anonymity include proxies, which channel communications through an intermediary device. Not all proxies provide anonymity, even if they can help journalists access information online that was previously censored. In addition, not all proxies utilize encryption and those that do, do not necessarily provide anonymity.

digital security trainings in newsrooms and journalism school curricula.[37] The proposed amendment would undermine these best practices because a journalist using anonymization tools could be the target of a remote access warrant to obtain evidence, even if that person is not suspected of criminal activity.

Tor and other anonymizing proxies are widely used by journalists seeking to protect their communications and their sources. These tools are critical for journalists to protect their communications with sources and to carry out their constitutionally recognized role. As currently written, the proposed amendment to Rule 41 could detrimentally impact journalists and erode the confidentiality of their relationships with sources, even when using Tor or other anonymizing tools to obscure identifying information.

II. Methods for infecting computers with malware can compromise the credibility of news media.

The proposed amendment to Rule 41 also fails to appropriately address the manner in which law enforcement can perform remote access searches. News organizations have been used as "covers" for the installation of malware. The impersonation of the news media in order to execute a remote access search contemplated by the proposed amendment to Rule 41 is unacceptable.

Law enforcement can deliver malicious software to their targets in numerous ways. One way is through a watering hole attack, which occurs when custom malicious code is installed on a website that is popular with the target group and which infects the computers of everyone who visits the site.[38] The FBI, non-state actors, and foreign governments have used this method to surveil sources.[39] A few years ago, the website for the Council on Foreign Relations was the victim of a watering-hole attack.[40] More recently, advertising on the website for Forbes magazine was compromised, resulting in the installation of malware on readers' computers.[41]

Another delivery method for malware is through social engineering, or the practice of obtaining confidential information by the manipulation of legitimate users. In

---

[37] *See, e.g.*, Frank Smyth, *Digital Security Basics for Journalists*, Medill National Security Zone, http://bit.ly/LeuRpv; Susan E. McGregor, *Digital Security and Source Protection for Journalists*, Columbia Journalism School (2014), http://bit.ly/1Abz0PT; Chris Walker and Carol Waters, *Learning Security: Information Security Education for Journalists*, Tow Center for Digital Journalism at Columbia Journalism School (Feb. 5, 2015), http://bit.ly/1BXZqCR; Pew Research Center, *Investigative Journalists and Digital Security: Perceptions of Vulnerability and Changes in Behavior* (Feb. 5, 2015), http://pewrsr.ch/1DPwQ9b.

[38] *See, e.g.,* Threat Encyclopedia, TrendMicro, http://bit.ly/1zX6Klf.

[39] *See, e.g.*, Kevin Poulsen, *Visit the Wrong Website, and the FBI Could End Up in Your Computer*, Wired (Aug. 5, 2014), *available at* http://wrd.cm/1As2qfV; see also Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, Wired (Sept. 13, 2013), *available at* http://wrd.cm/1v11NYi.

[40] Michael Mimoso, *Council on Foreign Relations Website Hit by Watering Hole Attack, IE Zero-Day Exploit*, Threatpost (Dec. 29, 2012), *available at* http://bit.ly/1zgXAfE.

[41] Thomas Fox-Brewster, *Forbes.com Hacked In November, Possibly By Chinese Cyber Spies*, Forbes.com (Feb. 10, 2015, 6:44 P.M.), http://onforb.es/1CgbMZw.

2007, the Federal Bureau of Investigation impersonated the Associated Press (the "AP") in order to deliver malware surreptitiously to a criminal suspect in the course of an investigation and thereby trace his location.[42] The FBI sought review from the Office of General Counsel ("OGC") and obtained a Title III warrant from a magistrate judge.

In that case, FBI agents sent a fake AP article to a target suspected of making bomb threats to his school. Once the target clicked on the link, he unknowingly downloaded sophisticated malware, which revealed his computer location and Internet Protocol address, and which helped agents confirm his identity.[43] While the FBI did seek the appropriate warrants it appears that the FBI failed to notify the OGC and the judge that the malware was delivered in the guise of an AP article, with an AP byline, and therefore impersonated a news media organization.

In response, the AP demanded that the FBI cease its impersonation of the news media. AP President and CEO Gary Pruitt said, "In stealing our identity, the FBI tarnishes that reputation, belittles the value of free press rights enshrined in our Constitution and endangers AP journalists and other newsgatherers around the world…[t]his deception corrodes the most fundamental tenet of a free press—our independence from government control and corollary responsibility to hold government accountable."[44] Ultimately, this type of action "erodes our ability to gather news by intimidating sources who might otherwise speak freely with our journalists."[45]

In addition to lacking any safeguards for First Amendment activity, and undermining existing statutory and constitutional protections, the proposed amendment to Rule 41 turns a blind eye to the threat of law enforcement impersonation of the news media in an effort to execute a remote access search. The interests protected by the First Amendment demand that law enforcement not impersonate the news media to facilitate remote access searches. However, under the proposed amendment to Rule 41, law enforcement is not required to disclose how it plans to execute a search when it applies for a remote access warrant. It would be impossible for a judge presented with a request to issue a warrant for a remote access search to understand that First Amendment rights may be implicated, thereby triggering the "scrupulous exactitude" requirement of

---

[42] Mike Carter, *FBI confirms it used fake story, denies bogus Times Web link*, Seattle Times (Oct. 28, 2014), *available at* http://bit.ly/1DZSbNR.

[43] See e.g., Ellen Nakashima and Paul Farhi, *FBI Lured Suspect with Fake Web Page, but May Have Leveraged Media Credibility*, Wash. Post (Oct. 28, 2014), *available at* http://wapo.st/1xCpHpk; *see also* Eric Tucker, *Associated Press Demands FBI Never Again Impersonate Media*, Huffington Post, (Nov. 10, 2014), *available at* http://huff.to/1MovNmw.

[44] Tucker, *supra* n.42.

[45] *Id*. As the Reporters Committee stated in a letter to the Attorney General and FBI Director, sent on behalf of 26 media organizations concerning the FBI's impersonation of the AP, using the news media as a cover for remote access searches "endangers the media's credibility and creates the appearance that the media is not independent of the government. It undermines media organizations' ability to independently report on law enforcement. It lends itself to the appearance that media organizations are compelled to speak on behalf of the government." Reporters Comm. for Freedom of the Press, Ltr. to Attorney General Holder and FBI Director Comey (Nov. 6, 2014), *available at* http://www.rcfp.org/sites/default/files/2014-11-06-letter-to-doj-fbi-regarding-se.pdf.

Stanford Daily. The omission of these safeguards risks treading on vital First Amendment rights.

The proposed amendment to Rule 41 implicates constitutional and statutory rights of journalists and news media organizations in myriad ways that must be addressed by Congress if they are to be altered. Given the host of legal and policy considerations raised by the proposed amendment to Rule 41, the Reporters Committee urges the Committee to reject the proposed language in full.

Sincerely,

Bruce D. Brown, Esq.
Katie Townsend, Esq.
Hannah Bloch-Wehba, Esq.
Jennifer Henrichsen
Reporters Committee for Freedom of the Press