Testimony and Statement for the Record of

Alan Butler
Senior Counsel
Electronic Privacy Information Center

on

Proposed Amendments to Rule 41
of the Federal Rules of Criminal Procedure

before the

Judicial Conference Advisory Committee on Criminal Rules

November 5, 2014

Judge Raggi, Members of the Advisory Committee on the Federal Rules of Criminal Procedure, thank you for the opportunity to participate in today's hearing on the proposed amendments. My name is Alan Butler and I am Senior Counsel at the Electronic Privacy Information Center ("EPIC").

EPIC is a non-partisan research organization in Washington, D.C., established in 1994 to focus public attention on emerging privacy and civil liberties issues.[1] We work with a distinguished panel of advisors in the fields of law, technology, and public policy.[2] EPIC has previously filed *amicus* briefs in cases concerning the core procedural protections granted under the Fourth Amendment: notice and the opportunity to challenge the scope of a government search. For example, in 2002 EPIC filed a brief in *United States v. Bach*, arguing that the Fourth Amendment requires officer presence during the execution of a warrant and that it was therefore unlawful to serve a warrant on an Internet Service Provider via facsimile.[3]

EPIC has a particular interest in ensuring that Fourth Amendment privacy rights are not eroded by the use of emerging surveillance technologies. As Justice O'Connor famously addressed in *Arizona v. Evans*, "[w]ith the benefits of more efficient law enforcement mechanisms comes the burden of corresponding constitutional responsibilities."[4] In an effort to maintain these constitutional responsibilities, EPIC routinely participates as *amicus curiae* in major Supreme Court cases addressing Fourth Amendment rights in the context of emerging technologies.

For example, in 2011 EPIC, joined by thirty legal scholars and technical experts, filed a brief in *United States v. Jones*, arguing that the use of invasive GPS tracking systems is a search requiring a warrant under the Fourth Amendment.[5] The Court ultimately found that the warrantless installation and use of a GPS device to track an individual over 30 days violated the Fourth Amendment.[6] In 2012, EPIC, joined by thirty-two legal scholars and technical experts, as well as eight transparency organizations, filed a brief in *Clapper v. Amnesty International, USA*, arguing that the NSA's Signals Intelligence capabilities have expanded to the point where it would be reasonable for United States persons to assume that all of their communications sent abroad are being routinely collected.[7]

In 2013, EPIC, joined by twenty-four legal scholars and technical experts, filed a brief in *Riley v. California*, arguing that modern cell phones provide access to a wealth of sensitive

---

[1] *About EPIC*, EPIC, https://epic.org/epic/about.html.
[2] *EPIC Advisory Board*, EPIC, http://epic.org/epic/advisory_board.html.
[3] *See* Brief of *Amicus Curiae* EPIC in Support of Appellee, United States v. Bach, 310 F.3d 1063 (8th Cir. 2002) (No. 02-1238).
[4] 514 U.S. 1, 17-18 (1995); *see also EPIC, Sandra Day O'Connor's Legacy*, https://epic.org/privacy/justices/oconnor/.
[5] *See* Brief of *Amici Curiae* EPIC and Legal Scholars and Technical Experts in Support of the Respondent, United States v. Jones, 132 S. Ct. 945 (2012) (No. 10-1259).
[6] *Jones*, 132 S. Ct. at 949.
[7] *See* Brief of *Amici Curiae* EPIC, Thirty-two Technical and Legal Scholars, and Eight Transparency Organizations in Support of Respondents, Clapper v. Amnesty Int'l, USA, 133 S. Ct. 1138 (2013) (No. 11-1025).

personal data and that phones should not be subject to warrantless searches incident to arrest.[8] In *Riley*, the Court unanimously held that officers may not search the contents of a cell phone without a warrant, even where that phone is seized during a lawful arrest.[9] The Court in *Riley* addressed the importance of the procedural protections established by the Fourth Amendment. Rejecting the government's argument that law enforcement protocols would suffice to limit access to certain sensitive information, the Court emphasized that "the Founders did not fight a revolution to gain the right to government agency protocols."[10] The Court also found that cell phone searches could be particularly invasive because they would allow the inspection of remotely stored files.[11]

We appreciate the Committee's important work in maintaining the Federal Rules of Criminal Procedure. In my statement today, I will: (1) describe the history of two key Fourth Amendment requirements relevant to Rule 41: notice and officer presence upon execution of a warrant; (2) discuss the history of and limitations on "covert entry" warrants; and (3) recommend that the proposed amendment not be adopted because it would authorize unreasonable law enforcement practices and inhibit the development of Fourth Amendment standards for remote access searches.

I. It is Well Established That Notice, Officer Presence, and Other Formalities Are Key to Fourth Amendment Reasonableness

The Fourth Amendment was adopted to ensure that there were procedural safeguards against the arbitrary exercise of governmental authority, "securing to the American people, among other things, those safeguards which had grown up in England to protect the people from unreasonable searches and seizures . . . ."[12] The Supreme Court's decision in *Weeks v. United States* heralded the dawning of the age of constitutional criminal procedure, in which the Court established the exclusionary rule, prohibiting introduction of evidence obtained in violation of the Fourth Amendment, and identified the core practices and formalities that now circumscribe lawful searches. The exclusionary rule was essential to the protection of Fourth Amendment rights because introduction of unlawfully obtained evidence at trial would "affirm by judicial decision a manifest neglect if not an open defiance of the prohibitions of the Constitution, intended for the protection of the people against such unauthorized action."[13]

The Court in *Weeks* recognized that prohibiting the government's use of improperly obtained evidence was necessary to ensure that the formalities and procedural safeguards required by the Fourth Amendment were followed. "The effect of the 4th Amendment is to put the courts of the United States and Federal officials, in the exercise of their power and authority, under limitations and restraints as to the exercise of such power and authority. . . ."[14] Relaxing

[8] *See* Brief of *Amicus Curiae* EPIC and Twenty-four Technical Experts and Legal Scholars in Support of Petitioner, Riley v. California, 134 S. Ct. 2473 (2014) (No. 13-132).
[9] *Riley*, 134 S. Ct. at 2494.
[10] *Id*. at 2491.
[11] *Id*. (citing Brief for Electronic Privacy Information Center in No. 13-132, at 12-14, 20).
[12] Weeks v. United States, 232 U.S. 383, 391 (1914).
[13] *Id.* at 394.
[14] *Id.* at 393.

well-established procedures would lead to "gradual depreciation of the rights secured by [the Fourth Amendment] by imperceptible practice of courts or by well-intentioned but mistakenly over-zealous executive officers."[15]

Even where an officer conducts a search pursuant to an authorized warrant, the Fourth Amendment requires that certain procedural formalities be followed to protect against abuse. Since the 1700s, United States law has required an officer's presence during the service of a search warrant.[16] An officer's presence discourages government abuse of power and unwarranted intrusion upon privacy by ensuring guarantees of trustworthiness and accountability. The Supreme Court has long recognized the importance of strict adherence to procedural safeguards in the execution of search warrants, because "[i]t may be that it is the obnoxious thing in its mildest and least repulsive form; but illegitimate and unconstitutional practices get their first footing . . . *by silent approaches and slight deviations from legal modes of procedure*."[17] Therefore, "[i]t is the duty of the courts to be watchful for the constitutional rights of the citizen, and against any stealthy encroachment thereon."[18]

But officer presence alone is not sufficient to make the service of a warrant reasonable under the Fourth Amendment; the method of entry into the place to be searched is also an important consideration. As the Supreme Court stated, "we have little doubt that the Framers of the Fourth Amendment thought that the method of an officer's entry into a dwelling was among the factors to be considered in assessing the reasonableness of a search or seizure."[19] In fact, the Court has held that notice provided in advance of a search is an important element of Fourth Amendment reasonableness.

In *Wilson v. Arkansas*, the Court found that advanced notice was a clearly established requirement of a reasonable search based on the common law history and practice.[20] The Court also found that its own cases supported the principle of prior notice as being "embedded in Anglo-American law."[21] The Court unanimously held that the "common-law 'knock and announce' principle forms a part of the reasonableness inquiry under the Fourth Amendment," specifically stating that "an officer's unannounced entry into a home might be unreasonable under the Fourth Amendment."[22]

Notice, officer presence, and other formalities are necessary to guarantee accountability and trustworthiness in the exercise of police power. As the Supreme Court has emphasized, "[t]he value judgment that [has historically] motivated a united democratic people fighting to defend those very freedoms from totalitarian attack is unchanged."[23] Procedural formalities are

---

[15] Gouled v. United States, 255 U.S. 298, 304 (1921).
[16] *See* Boyd v. United States, 116 U.S. 616, 624 (1886) (detailing the history of search and seizure law and procedure).
[17] *Boyd*, 116 U.S. at 633. (emphasis added).
[18] *Id.*
[19] Wilson v. Arkansas, 514 U.S. 927, 934 (1995).
[20] *Id.* at 931.
[21] *Id.* at 934 (quoting Miller v. U.S. 357 U.S. 301, 313 (1958)).
[22] *Id.* at 929, 934.
[23] Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Vill. of Stratton, 122 S. Ct. 2080, 2091 (2002).

critical in preserving our privacy in order to maintain cherished values of humanity and civil liberty. In *McVeigh v. Cohen*, which addressed unauthorized access to electronic communications, the court stated:

> In these days of "big brother," where through technology and otherwise the privacy interests of individuals from all walks of life are being ignored or marginalized, it is imperative that statutes explicitly protecting these rights be strictly observed.[24]

Fundamental principles "established by years of endeavor and suffering" cannot be sacrificed to the needs or convenience of law enforcement."[25] Notice and officer presence are key elements of reasonableness under the Fourth Amendment and courts should only allow deviation from these requirements with caution and under very strict and limited conditions.

II. Courts Have Only Allowed Delayed Notice and Permitted Covert Entry Warrants in Limited Circumstances

In certain limited circumstances, courts have held that law enforcement officers may execute search warrants through covert means and without prior notice to the subject.[26] The authority to conduct "surreptitious searches and seizures"[27] has been limited to cases where (1) delayed notice and covert entry is necessary, and (2) notice will be provided within a reasonable time after the search.[28] This is consistent with the Supreme Court's holding that notice is an element of Fourth Amendment reasonableness.[29]

The judicial authorization of surreptitious searches, initiated without prior notice to or confrontation of the subject, is a relatively new development in the history of Fourth Amendment law. Covert entry warrants were not contemplated during the founding era, and no published opinions in the United States addressed them until 1985. In *United States v. Frietas*, the Ninth Circuit found the Fourth Amendment requires that "surreptitious entries be closely circumscribed."[30] Drawing on the limitations on wiretapping outlined in Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-2520, the court in *Frietas* found that both "the necessity for the surreptitious seizure and the subsequent notice" were an important element of the Fourth Amendment reasonableness analysis.[31]

The Ninth Circuit in *Frietas* noted that the Fourth Amendment does not prohibit all surreptitious entries, as the Supreme Court's held in *Dalia v. United States*,[32] but that "absence of

---

[24] 983 F. Supp. 215, 220 (D.D.C. 1998).
[25] *Weeks*, 232 U.S. at 393.
[26] *See* Jonathan Witmer-Rich, *The Rapid Rise of Delayed Notice Searches, and the Fourth Amendment "Rule Requiring Notice,"* 41 Pepp. L. Rev. 509, 519-25 (2014).
[27] Also referred to as "sneak and peek" or "sneak and steal" warrants.
[28] *See* United States v. Villegas, 899 F.2d 1324, 1337 (2d Cir. 1990).
[29] Wilson v. Arkansas, 514 U.S. 927, 929 (1995).
[30] United States v. Frietas, 800 F.2d 1451, 1456 (9th Cir. 1985).
[31] *Id*.
[32] 441 U.S. 238 (1979).

any notice requirement in the warrant casts strong doubt on its constitutional adequacy."[33] The Court in *Dalia* rejected a defendant's argument that officers' covert entry into his office to install "bugging equipment" violated the Fourth Amendment.[34] The Court found that "[t]he Fourth Amendment does not prohibit *per se* a covert entry performed for the purpose of installing otherwise legal electronic bugging equipment."[35] However, in its finding that the surreptitious entry was constitutional, the Court relied upon the lower court finding that the "safest and most successful method of accomplishing the installation of the wiretapping device was through breaking and entering [the office]."[36] The Court also found that delayed notice equivalent to that provided under Title III would be a "constitutionally adequate substitute for advance notice" in the case of a covert entry warrant.[37]

The U.S. Court of Appeals for the Second Circuit later addressed the validity of surreptitious search warrants in a series of cases beginning in 1990. In *United States v. Villegas*, the Second Circuit considered a defendant's challenge to a surreptitious search of his farmhouse, executed pursuant to a warrant but without notice until his arrest two months later.[38] The court found that "certain safeguards are required where the entry is to be covert," but concluded "appropriate conditions were imposed" in that case.[39] Specifically, the court found that "two limitations on the issuance of warrants for covert-entry searches for intangibles are appropriate."[40] The first requirement is that officers show a "reasonable necessity" for not providing advance notice of the search.[41] The second requirement is that delayed notice must be given "within a reasonable time after the covert entry."[42] The court agreed with the Ninth Circuit's finding in *Frietas* that "as an initial matter, the issuing court should not authorize a notice delay of longer than seven days," but may grant extensions thereafter based on a "fresh showing of the need for further delay."[43] Subsequent lower court decisions, addressing covert entry warrants, have failed to recognize that notice is an important element of Fourth Amendment reasonableness, as the Supreme Court found in *Wilson v. Arkansas*.[44]

Congress later authorized the issuance of delayed notice warrants in Section 213 of the USA PATRIOT Act, but only in certain circumstances.[45] The law includes three express limitations on the issuance of delayed notice warrants, similar to those imposed by the Ninth Circuit in *Freitas* and the Second Circuit in *Villegas*: first, the issuing court must find "reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result," second, the warrant must prohibit the seizure of tangible property and electronic files, "except where the court finds reasonable necessity for the seizure,"

---

[33] *Frietas*, 800 F.2d 1456.
[34] *Dalia*, 441 U.S. at 241-42.
[35] *Id*. at 248.
[36] *Id*. at 248 n.8.
[37] *Id*. at 248.
[38] 899 F.2d 1324, 1336 (2d Cir. 1990).
[39] *Id*.
[40] *Id*. at 1337.
[41] *Id*.
[42] *Id*.
[43] *Id*.
[44] *See* Witmer-Rich, *supra*, at 524 n.86.
[45] 18 U.S.C. § 3103a.

and finally, the warrant must provide for notice within a "reasonable period not to exceed 30 days."[46] Prior to the enactment of the Patriot Act, some courts had held that the failure to provide notice is not *per se* unconstitutional,[47] but these decisions do not fully address the fact that notice is a core element of Fourth Amendment reasonableness, as the Court found in *Wilson*.

Existing precedents do not support the conclusion that surreptitious warrants may be issued without first establishing that delayed notice is necessary and providing for future notice within a reasonable period of time.

III. The Proposed Amendment to Rule 41 Would Depart from Established Precedent and Inhibit the Future Fourth Amendment Development

Because it would authorize the issuance of digital surreptitious search warrants without requiring a showing that such methods are necessary or that notice be given within a reasonable amount of time after the search, the proposed amendment to Rule 41 would be inconsistent with well-established Fourth Amendment precedents.

The rule would grant magistrates the authority to "issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information" if either (1) "the district where the media or information is located has been concealed through technological means" or (2) "in an investigation of a violation of 18 U.S.C. § f1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts."

An officer applying for a remote access warrant under the proposed revision of Rule 41 would not have to make any showing that the delay in notifying the target of the search is reasonably "necessary" for the investigation. Rather, the Rule would authorize issuance of a surreptitious search warrant in any case where the target of the search has used an online proxy tool. There may be some cases where a court would find it is reasonably necessary to use remote access tools, but that will not be the case in every instance where the target is using a proxy service. Without a requirement that the requesting officer establish necessity as required for all other covert search warrants, the proposed rule will be overbroad.

Furthermore, the proposed amendment to Rule 41(f)(1) would not require an officer to provide notice within a reasonable time. Instead, the rule would require that the officer "make reasonable efforts" to serve a copy of the warrant. That is certainly necessary, but it is not sufficient, as the Court established in *Wilson* and circuit courts recognized in *Frietas* and *Villegas*. Even the delayed notice provision in the Patriot Act, which has been widely criticized for being overbroad, provides for notice within a "reasonable period not to exceed 30 days," with a requirement that any further extensions be independently justified.

---

[46] 18 U.S.C. § 3103a(b).

[47] *See*, *e.g.*, United States v. Simons, 206 F.3d 392, 402-03 (4th Cir. 2000); United States v. Pangburn, 983 F.2d 440, 455 (2d Cir. 1993).

As drafted, the amended Rule 41 would authorize the issuance of overly broad covert search warrants and would not require sufficiently prompt notice to satisfy Fourth Amendment scrutiny.[48]

The proposed amendments to Rule 41 would not only be constitutionally defective, they would also inhibit development of Fourth Amendment law in the area of remote electronic searches. Fourth Amendment law develops primarily through suppression motions filed by defendants in response to the use of new law enforcement techniques.[49] However, this process breaks down where the exclusionary rule is not available as a remedy to the defendants who might seek to challenge a new investigative technique.[50] The exclusionary rule is not an available remedy when the officer relied in good faith upon a warrant issued by a magistrate, even when that warrant is later deemed invalid.[51]

It would therefore be improper to grant new warrant authority by amending Rule 41 without first establishing that proposed rule is consistent with the Fourth Amendment. Future defendants who are subject to a search authorized under the amended rule would have no available remedy, and therefore no incentive to challenge potentially unconstitutional intrusions into their computer networks. In that case, the amendment itself would resolve the constitutional question before it is properly presented in an individual case.

Conclusion

The proposed amendments to Rule 41 would authorize searches beyond the scope permissible under the Fourth Amendment. Specifically, the rule would allow for surreptitious searches without the required showing of necessity, and the resulting warrants would not include the requirement that notice be served within a reasonable time after the search. For these reasons, the Committee should not adopt the proposed amendments as drafted.

Thank you for the opportunity to participate in today's hearing. I will be pleased to answer your questions.

[48] For example, the Seattle Times recently reported that the FBI used a link to a fake version of the newspaper's webiste to remotely install surveillance software on a suspect's computer. Mike Carter, *FBI Created Fake Seattle Times Web Page to Nab Bomb-threat Suspect*, (Oct. 27, 2014), http://seattletimes.com/html/localnews/2024888170_fbinewspaper1xml.html. The FBI special agent in charge was quoted as saying the FBI only uses remote access techniques "when there is sufficient reason to believe it could be successful in resolving a threat." *Id*.

[49] Orin Kerr, *Good Faith, New Law, and the Scope of the Exclusionary Rule*, 99 Geo. L. J. 1077, 1090 (2011).

[50] *Id*. at 1092-95.

[51] *See* United States v. Leon, 468 U.S. 897, 925 (1984).