No. 13-30077
[NO. CR12-119MJP, USDC, W.D. Washington]

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff-Appellee,

v.

MICHAEL DREYER,
Defendant-Appellant.

PETITION OF UNITED STATES FOR REHEARING

Appeal from the United States District Court
for the Western District of Washington at Seattle
The Honorable Marsha J. Pechman
United States District Judge

ANNETTE L. HAYES
Acting United States Attorney
Western District of Washington

HELEN J. BRUNNER
Assistant United States Attorney
700 Stewart Street, Suite 5220
Tacoma, Washington 98402
Telephone: 206-553-7970

Of Counsel:
SCOTT A.C. MEISLER
Criminal Division, Appellate Section
U.S. Department of Justice

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Supreme Court Cases

Circuit Court Cases

Federal Statutes

Miscellaneous

PRELIMINARY STATEMENT

In *United States v. Dreyer*, 767 F.3d 826 (9th Cir. 2014), a panel of this Court held that the regulations extending the Posse Comitatus Act (PCA) to Navy military personnel also applied to Naval Criminal Investigative Service (NCIS) civilian employees and that an NCIS special agent violated these regulations by using a law enforcement program to identify child pornography publicly offered for download from computers using publicly available peer-to-peer software. Because three NCIS agents conducted similar searches on multiple occasions, a majority of the panel concluded these violations of the act were widespread and required suppression of child pornography found during the resulting search of Michael Dreyer's computer. This opinion overlooks and misapprehends several key factual and legal issues. Therefore, the United States respectfully requests this Court to rehear the case.

First, the conclusion that the PCA-like restrictions apply to the NCIS agents overlooks the fact that the statute directing the Secretary of Defense to extend the PCA restrictions to the Navy limits its reach to military "members," and not civilian employees. *See* 10 U.S.C. § 375. Further, the opinion wrongly concludes the role of the NCIS Director as a Special Assistant to the Chief of Naval Operations creates a supervisory reporting relationship, rather than the advisory relationship that actually exists.

Second, and more importantly, the RoundUp program did not permit the agent to see anything that a computer user did not affirmatively place into a "share" (and

therefore public) file after installing the peer-to-peer program on the computer. As this Court has held, a defendant's expectation of privacy does not "survive [his] decision to install and use file-sharing software, thereby opening his computer to anyone else with the same freely available program." *United States v. Ganoe*, 538 F.3d 1117, 1127 (9th Cir. 2008). This fact, plus the fact that another appellate court—albeit in a non-precedential decision—concluded that NCIS agents did not violate the PCA by engaging in such an investigation, establishes that suppression was not warranted. In April 2011, the NCIS agent had a good-faith belief that this investigative activity was within the scope of his authority. This Court's precedential finding that the conduct, in fact, violated the PCA is sufficient to deter any further NCIS investigations of this nature without the substantial societal cost of suppressing evidence where no constitutional (or even statutory) violation has taken place.

Finally, this Court applied a suppression remedy in this case without considering the important antecedent question of whether suppression is even authorized for violations of PCA-type restrictions that do not otherwise implicate constitutional rights. Suppression in this context is contrary to Supreme Court and Ninth Circuit precedent governing the exclusionary rule and improperly provides a suppression remedy for a violation of a regulation which does not involve a violation of a constitutional right. For all of these reasons, rehearing is appropriate.

FACTUAL AND PROCEDURAL BACKGROUND

In December 2010, three NCIS special agents began investigating the computer trade and distribution of child pornography using a software program called RoundUp. ER_113. The RoundUp program is a tool created to permit law enforcement officers to identify the Internet Protocol (IP) addresses [1] used by computers offering child pornography for download on publicly available peer-to-peer file-sharing programs. ER_113-14, 173. The program does not involve hacking into a target's computer; rather, RoundUp only permits a law enforcement officer to identify digital files containing child pornography that an individual has affirmatively placed in a "share" file after intentionally loading the peer-to-peer software on his or her computer. ER_115-117, 173. The program does not permit access to other private areas of a person's computer, or to files the user has not placed into the "share" file. ER_343.

To use the program, an agent first types in search terms commonly identified with child pornography. ER_17, 344. The program then searches for file names containing these search terms located in the "share" files on computers using public available peer-to-peer networks within the designated geographic area. ER_344.

[1] An individual does not have a reasonable expectation of privacy in a computer IP address because such addresses "are voluntarily turned over in order to direct the third party's servers." *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008). *See also United States v. Christie*, 624 F.3d 558, 573 (3d Cir. 2010)(same).

When a computer offering such a file is located, the program identifies the IP address used by the computer, ER_117, and shows its general geographic location. ER_344. No other identifying information about the user is provided. ER_117. RoundUp uses a library of hash values for known child pornography images and video files to determine whether any of the "share" files containing the search terms are known child pornography files. ER_126-127. The agent can then download the offered image and seek from the service provider the identity of the user to whom that IP address was assigned at that date and time.

On April 14, 2011, NCIS Special Agent Steve Logan logged on to the RoundUp program, and set the geographic parameters in the program to limit his searches to computers using IP addresses located within Washington State, a state with multiple military bases. ER_339, 360-62. Other than setting geographic limits, Logan could not further limit his search to shared files on computers or devices associated with active duty military members. ER_360-62.

RoundUp identified a computer in Washington State that had twenty files to share that had titles containing Logan's search terms. ER_120-21. Logan downloaded three files identified as known child pornography, including a three-minute and nineteen-second video. ER_132-34, 344, 349-52. Logan then requested the NCIS liaison at the National Center for Missing and Exploited Children to seek an administrative subpoena for the name and address of the subscriber using the

IP address at that date and time. ER_139-140, 353-54. That subscriber was Dreyer. ER_142, 354.

Because Dreyer was not an active-duty military member, Logan's report was forwarded to a local law enforcement officer who later obtained a search warrant for Dreyer's computer based on the information Logan provided. Logan's part in the investigation then ended. He had no involvement in the searches that followed, and never spoke with local law enforcement officers about the investigation.

Based on the evidence subsequently discovered during the execution of the search warrants, Dreyer was charged with both distribution and possession of child pornography. ER 482-484. He moved to suppress the evidence discovered on his computer, CR_17, 18, later arguing that suppression was required because Logan did not have lawful authority to investigate child pornography offenses under the Posse Comitatus Act, 18 U.S.C. § 1385. CR_25 at 6. The district court denied the motion to suppress the evidence after an evidentiary hearing. ER_60-65. Following a jury trial, Dreyer was convicted of all charges, his second federal conviction for child pornography offenses.

THE DECISION OF THIS COURT

A partially divided panel of this Court reversed. *Dreyer*, 767 F.3d at 837. The panel held that "the NCIS agent's investigation constituted improper military enforcement of civilian laws" and that the evidence collected as a result of that investigation should be suppressed. *Id.* at 827.

The panel acknowledged that the PCA does not refer to the Navy, and that "'PCA-like restrictions'" reach the Navy only via a non-penal statute, 10 U.S.C. § 375, and "as a matter of Department of Defense (DoD) and Naval policy." 767 F.3d at 830. The panel rejected, however, various grounds for concluding that the PCA-like restrictions do not apply to the NCIS agents in this case. The Court read *United States v. Chon*, 210 F.3d 990 (9th Cir. 2000), as foreclosing the argument that the NCIS agents are exempt from the restrictions because they are part of an agency headed by a civilian director with a civilian chain of command. *Dreyer*, 767 F.3d at 830-31. The panel also concluded that *Chon* remained controlling despite an intervening change in the NCIS command structure, pointing to the NCIS Director's role as "Special Assistant for Naval Investigative Matters and Security to the Chief of Naval Operations." *Id.* at 831.

The Court also rejected the argument that Logan's actions constituted indirect assistance to law enforcement that did not "subject civilians to [the] use [of] military power that is regulatory, prescriptive, or compulsory," because Logan's actions were not limited to supporting an on-going investigation into Dreyer's activities but rather constituted actions of "an independent actor who initiated and carried out this activity." *Id.* at 833. The Court further rejected any suggestion that there was an independent military purpose for Logan's investigation because Logan's investigation involved all computers in Washington State using peer-to-peer networks, and could not be otherwise limited to military personnel. *Id.* at 833-35. The Court found that

because of "the lack of any reasonable connection between the military and the crimes that Agent Logan was investigating," the Court concluded that his actions "violated the regulations and policies proscribing direct military enforcement of civilian laws." *Id.* at 835.

Having found a violation, a majority of the panel concluded there was a need to suppress the evidence to deter future PCA violations because the record showed that NCIS agents routinely engage in "broad surveillance activities that violate the restrictions on military enforcement of civilian law," and characterized Logan's activities as "surveillance of all the civilian computers in an entire state." 767 F.3d at 836. Because the record disclosed that Logan and two other NCIS agents had been involved in similar investigations over the course of several months, the Court found the violations to be widespread, and concluded that suppression was warranted because the government's litigating position also demonstrated "a profound lack of regard for the important limitations on the role of the military in our civilian society." *Id.*

Judge O'Scannlain dissented on the remedial issue. *Id.* at 838-42. He determined that suppression was inappropriate "[g]iven the significant costs of exclusion in PCA cases, as well as the meager evidence of PCA violations contained in the record." *Id.* at 842. While "not question[ing]" the suggestion in this Court's prior cases "that application of the exclusionary rule in the PCA context could be justified," Judge O'Scannlain noted "that there is a strong argument to be made that exclusion is

never justified for violations of the PCA," and that "[s]everal considerations" would support that argument. *Id.* at 841 n.3.

ARGUMENT

I. The Posse Comitatus Act Does Not Apply to the Civilian Special Agents of the Naval Criminal Investigative Service.

The PCA makes it a crime to "willfully use any part of the Army or the Air Force as a posse commitatus or otherwise to execute the laws in cases" "except in cases and under circumstances expressly authorized by the Constitution or Act of Congress." 18 U.S.C. § 1385. By its terms, the PCA does not apply to the Navy. Rather, in 1981, Congress passed a separate non-penal statute directing the Secretary of Defense to "prescribe such regulations as may be necessary to ensure that any activity" under Title 10 "does not include or permit direct participation by any *member* of the Army, Navy, Air Force or Marine Corps in a search, seizure, arrest, or other similar activity unless participation in such activity by such *member* is otherwise authorized by law." 10 U.S.C. § 375 (emphasis added). The term "member," as used in this statute, is reasonably understood as a term of art used throughout Title 10 to refer to enlisted, military personnel, and not civilians. *Cf. Vermont Agency of Natural Resources v. United States ex. Rel. Stevens*, 529 U.S. 765, 782-83 (2000)(referencing "the term of art 'member of an armed force' used throughout Title 10"). NCIS agents are civilian employees of the Navy. 10 U.S.C. § 7480. Thus, the statutory directive, by its terms, does not require the PCA-like restrictions to reach NCIS agents.

Moreover, the NCIS is not brought into the military command structure merely because the Director of the NCIS serves as a "Special Assistant for Naval Investigative Matters and Security to the Chief of Naval Operations." *Dreyer*, 767 F.3d at 831. To the contrary, in that role the NCIS Director acts merely as an advisor to the Chief of Naval Operations on investigations, law enforcement and security programs and does not create a line authority by the Chief of Naval Operations over the NCIS. *See* SECNAVINST 5430.107, paragraph 5; Add_34-35. The Court's conclusion to the contrary is in error.

II. Suppression Is Not Warranted to Deter Future Conduct.

In *United States v. Roberts*, 779 F.2d 565 (9th Cir. 1986), this Court concluded that the exclusionary rule should not be applied to a violation of the PCA unless it was necessary to deter future PCA violations where the record reflects "wide spread and repeated violations." Although finding the involvement by military personnel in a drug investigation was deliberate and in violation of PCA-like restrictions, the *Roberts* Court nonetheless noted that the violation was "unintentional and in good faith." *Roberts*, 779 F.2d at 568 (citing *United States v. Leon*, 468 U.S. 897 (1984)). The Court then rejected the defense arguments for suppression and dismissal of the indictment, observing that "the clear costs of applying an exclusionary rule are not countervailed by any discernible benefits." *Id.*

The *Roberts* Court relied on the Fourth Circuit's decision in *United States v. Walden*, 490 F.2d 372, 376-77 (4th Cir. 1974), a case which first suggested that a

suppression remedy might be available to address particularly widespread and egregious PCA violations. Nonetheless, the Fourth Circuit has since constrained *Walden* by clarifying that suppression is not a remedy for a PCA violation where the violative military operation did not involve the seizure of evidence. *United States v. Al-Talib*, 55 F.3d 923, 930 (4th Cir. 1995) (citing *United States v. Griley*, 814 F.2d 967, 976 (4th Cir. 1987)). The *Al-Talib* Court noted that this conclusion comports with the Supreme Court's command to restrict application of the exclusionary rule to "those areas where its remedial objectives are most efficaciously served." *Al-Talib*, 55 F.3d at 930 (quoting *United States v. Calandra*, 414 U.S. 338, 348 (1974)). Indeed, the opinion in this case is the only case in which a federal court actually suppressed evidence based on any form of PCA violation.

Here, to the extent there is a violation, it is of the regulation the Secretary of Defense adopted to implement 10 U.S.C. § 375. Although this Court may disagree that the changes to the NCIS command structure were sufficient to undermine the application of *Chon* to this case, the fact that the Navy believed the change sufficient establishes that the agents did not intentionally violate PCA restrictions. Logan's good faith is further supported by the fact that, on similar facts, the Sixth Circuit reached a conclusion contrary to that of this Court. See *United States v. Holloway*, 531 F. App'x. 582 (6th Cir. 2013). Although the decision is unpublished, it does suggest that the issue is one that was at least debatable and, therefore, that the agents had a good faith belief that their actions did not violate the PCA. Thus, this is not the

type of widespread violation that requires suppression of the evidence. To the contrary, the Court's finding of a violation is sufficient to deter any future investigative efforts of this type by NCIS agents. *Cf. United States v. Payner*, 447 U.S. 727, 733 n.5 (1980) (refusing to assume that lawless conduct similar to that of the IRS agents in the case "if brought to the attention of responsible officials, would not be dealt with appropriately").

More importantly, Logan's conduct here did not separately violate the Constitution. It amounted to nothing more than looking at files available to anyone seeking child pornography on a publicly available peer-to-peer network. *See United States v. Borowy*, 595 F.3d 1045, 1048 (9th Cir. 2010) (defendant's claim that he attempted to prevent LimeWire from sharing his files did not create an objectively reasonable expectation of privacy in the face of widespread public access); *United States v. Ganoe*, 538 F.3d 1117, 1127 (9th Cir. 2008). *See also United States v. Stults*, 575 F.3d 834, 843 (8th Cir. 2009)(same). This conduct did not involve surveillance or conduct that intruded on any information that was private. Thus, regardless of whether this Court finds a violation of the PCA-type restrictions, there was no violation of Dreyer's constitutional rights.

III. Suppression Is Not an Available Remedy for Violation of the PCA-Like Restrictions That Do Not Separately Violate Constitutional Rights.

The panel's decision to order suppression under *Roberts* is infected by an even more fundamental error. Specifically, whether suppression is appropriate to deter

violations of PCA-like restrictions first requires this Court to consider whether suppression is ever an appropriate remedy for such statutory or regulatory violations because the scope of this remedy must turn on why suppression is authorized. This in turn raises the antecedent question of whether suppression is ever authorized for a PCA violation.

The government did not previously raise this issue, but Judge O'Scannlain's dissent did. *See Dreyer*, 767 F.3d at 841 n.3. In *United States v. Grubbs*, 547 U.S. 90 (2006), the Supreme Court made clear that review of previously forfeited, but logically antecedent questions, is appropriate. The *Grubbs* Court considered a claim never raised or previously considered that was antecedent to the question on which certiorari had been granted. Specifically, before it turned to this Court's "conclusion that the [anticipatory] warrant at issue here ran afoul of the Fourth Amendment's particularity requirement," the Supreme Court "address[ed] the antecedent question whether anticipatory search warrants are categorically unconstitutional." *Id.* at 94. The Court noted that the latter issue was "'predicate to an intelligent resolution of the question presented,'" because it would "make little sense to address what the Fourth Amendment requires of anticipatory search warrants if it does not allow them at all." *Id.* at 94 & n.1 (quoting *Ohio v. Robinette*, 519 U.S. 33, 38 (1996)). Here, addressing the antecedent question of whether suppression is ever an available remedy for violating PCA-like restrictions is similarly warranted.

The answer to that antecedent question is no. Supreme Court and Ninth Circuit precedents draw a clear line between the availability of suppression as a remedy for constitutional violations (on the one hand) and statutory or regulatory violations (on the other). In *Sanchez-Llamas v. Oregon*, 548 U.S. 331 (2006), for example, the Court declined to create an exclusionary remedy for violations of the right to consular notification under a treaty. The Court recognized it has "applied the exclusionary rule primarily to deter constitutional violations" and "ha[d] suppressed evidence for statutory violations" in only a "few cases" where "the excluded evidence arose directly out of statutory violations that implicated important Fourth and Fifth Amendment rights" such as incriminating statements made following prolonged detention, and "suppression of evidence that was the product of a search incident to an unlawful arrest." *Id.* at 348; *see also United States v. Caceres*, 440 U.S. 741, 754-57 (1979)(declining to apply an exclusionary remedy to an agency's violation of its own regulations governing electronic eavesdropping).

Consistent with *Sanchez-Llamas*, this Court and others have held that "an exclusionary rule is typically available only for constitutional violations, not for statutory or treaty violations." *United States v. Lombera-Camorlinga*, 206 F.3d 882, 886 (9th Cir. 2000) (en banc). *Accord, e.g., United States v. Adams*, 740 F.3d 40, 43-44 (1st Cir. 2014) (declining to apply exclusionary rule to IRS agent's assumed violation of a statute and explaining that "statutory violations, untethered to the abridgment of constitutional rights, are not sufficiently egregious to justify suppression");

United States v. Abdi, 463 F.3d 547, 556-57 (6th Cir. 2006) (rejecting suppression for violation of a statutory administrative warrant requirement and explaining that "the exclusionary rule is an appropriate sanction for a statutory violation only where the statute specifically provides for suppression as a remedy or the statutory violation implicates underlying constitutional rights such as the right to be free from unreasonable search and seizure"). Moreover, this Court has held that an exclusionary remedy should not be read into a statutory scheme when Congress has prescribed a remedy other than exclusion, such as a criminal penalty against the violator. *See, e.g., United States v. Forrester*, 512 F.3d 500, 512-13 (9th Cir. 2008) (pen register statute); *United States v. Feng*, 277 F.3d 1151, 1154 (9th Cir. 2002) (prosecutor's alleged violation of criminal bribery statute); *United States v. Michaelian*, 803 F.2d 1042, 1049 (9th Cir. 1986) (IRS' unauthorized disclosure of tax return information).

Under these precedents, the exclusionary rule does not apply to violations of the PCA-like restrictions at issue here. The PCA itself prescribes criminal sanctions for certain military involvement in civilian law enforcement, not the exclusion of evidence. 18 U.S.C. § 1385. Accordingly, it "would 'encroach upon the prerogatives' of Congress" to supplement its chosen criminal sanction with the exclusion remedy. *See Forrester*, 512 F.3d at 512 (quoting *United States v. Frazin*, 780 F.2d 1461, 1466 (9th Cir. 1986)). If violation of the PCA does not give rise to an exclusionary remedy, then it follows that this remedy is unavailable for violations of the regulations resulting from the statute directing the Secretary of Defense to extend PCA-like

restrictions to the Navy. Nothing in the text of that statute — which directs the Secretary of Defense to act "as may be necessary" to avoid "direct participation" by the Armed Forces in civilian law enforcement activities — speaks in terms of excluding evidence. 10 U.S.C. § 375. Nor does the legislative history evince any Congressional preference for exclusion. The House Report reveals that Congress was aware of the uniform federal court precedents declining to apply the exclusionary rule to alleged PCA violations, and does not suggest that Congress disapproved of that result. H.R. Rep. No. 97-71, Part 2, at 5, 97th Cong., 1st Sess. (June 12, 1981).

Although an exclusionary remedy may be available when statutory violations "implicate[] important Fourth Amendment * * * interests," *see Sanchez-Llamas*, 548 U.S. at 348, no such interests are involved here. Instead, this Court's precedents confirm that Logan's use of RoundUp to find and download files from Dreyer's "share" files did not constitute a Fourth Amendment search because Dreyer had no expectation of privacy in files he offered to the world via a peer-to-peer file-sharing program. *See Borowy*, 595 F.3d at 1048; *Ganoe*, 538 F.3d at 1127. Therefore, the only violation here is a regulatory violation related to the affiliation of the law enforcement agent who conducted the initial investigation. That is both a far cry from the statutory violations described in *Sanchez-Llamas*, 548 U.S. at 348, and directly analogous to the "technical defect[s]" in arrest authority this Court and others have found to be an insufficient basis for excluding evidence. *See United States v. DiCesare*,

765 F.2d 890, 896-97 (9th Cir. 1985) (declining to apply exclusionary rule where federal officer allegedly lacked statutory authority to execute a state warrant, because the warrant's "validity would not be in question" if state officer executed it, and any defect was "merely a technical [one that] did not implicate any constitutional violations"); *United States v. Harrington*, 681 F.2d 612, 614-15 (9th Cir. 1982) (similar). *See also United States v. Ryan*, 731 F.3d 66, 68-69 & n.3 (1st Cir. 2013) (refusing to suppress fruits of an otherwise lawful "arrest made outside of a federal law enforcement officer's statutory jurisdiction").

Finally, suppression is all the more unwarranted because this case involves a perceived violation of agency regulations, not a statute. *See Dreyer,* 767 F.3d at 830-35. This Court, however, has held that "violation of an agency regulation does not require suppression of evidence" "[a]bsent a constitutional violation or a congressionally created remedy," both of which are lacking here. *United States v. Hinton*, 222 F.3d 664, 674 (9th Cir. 2000) (citation and quotation marks omitted); *see also United States v. Choate*, 619 F.2d 21, 23 (9th Cir. 1980). That standard follows from *Caceres*, where the Court explained that "rigid application" of the exclusionary rule to regulatory violations could discourage agencies from regulating the conduct of criminal investigations. 440 U.S. at 755-56. This case directly implicates that concern; the Navy's incentive to maintain what the panel believed to be broad restrictions against its employees participating in civilian law enforcement, 767 F.3d at 831-32, is reduced when any violation by a civilian employee can become a basis for suppression if a

court later deems the violation sufficiently widespread or deterrence-worthy. "[T]he result," in the words of *Caceres*, "might well be fewer and less protective regulations." 440 U.S. at 756. That disincentive does not dissolve because the Secretary of Defense must follow a Congressional directive to extend the PCA-like restrictions to the Navy. As noted above, this statute speaks in terms of "member[s]," 10 U.S.C. § 375, a "term of art" referring to enlisted military personnel, not civilians. *Cf. Vermont Agency of Natural Resources*, 529 U.S. at 782-83. If suppression is a remedy for violations of regulations, the Secretary might well prefer "to have no rules except those mandated by statute," *Caceres*, 440 U.S. at 756—that is, restrictions that apply only to "member[s]" of the Navy, not civilian NCIS Special Agents.

///

///

//

CONCLUSION

For the reasons stated above, the United States respectfully requests that this Court rehear the case and find that suppression is not warranted.

DATED this 18th day of November, 2014.

Respectfully submitted,

ANNETTE L. HAYES
Acting United States Attorney
Western District of Washington

/s/ Helen J. Brunner
HELEN J. BRUNNER
Assistant United States Attorney
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
Phone: 206-553-7970

Of Counsel:
SCOTT A.C. MEISLER
Criminal Division, Appellate Section
U.S. Department of Justice

CERTIFICATE OF COMPLIANCE
WITH WORD LIMIT

I certify that, pursuant to Circuit Rule 40-1, the attached the Petition for Rehearing is proportionately spaced, has a typeface of 14 points, and contains 4,191 words, less than the 4,200 allowed.

DATED this 18th day of November, 2014.

s/ Helen J. Brunner
HELEN J. BRUNNER
Assistant United States Attorney

CERTIFICATE OF SERVICE

I hereby certify that on November 18, 2014, I electronically filed the foregoing Petition for Rehearing of the United States with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

DATED this 18th day of November, 2014.

s/ Helen J. Brunner
HELEN J. BRUNNER
Assistant United States Attorney

767 F.3d 826, 14 Cal. Daily Op. Serv. 10,767, 2014 Daily Journal D.A.R. 12,668
(Cite as: 767 F.3d 826)

C

United States Court of Appeals,
Ninth Circuit.
UNITED STATES of America, Plaintiff–Appellee,
v.
Michael Allan **DREYER**, Defendant–Appellant.

No. 13–30077.
Argued and Submitted May 16, 2014.
Filed Sept. 12, 2014.

Background: A defendant was convicted in the United States District Court for the Western District of Washington, Marsha J. Pechman, Chief District Judge, of distributing child pornography, and possessing child pornography. The defendant appealed.

Holdings: The Court of Appeals, Berzon, Circuit Judge, held that:
(1) the restriction on military personnel providing direct assistance to civilian law enforcement applies to agents of the Naval Criminal Investigative Service (NCIS);
(2) a NCIS special agent violated the regulations and policies proscribing direct military enforcement of civilian laws; and
(3) the government's widespread and repeated violation of regulations and policies prohibiting military personnel providing direct assistance to civilian law enforcement warranted application of the exclusionary rule.

Reversed and remanded.

Kleinfeld, Senior Circuit Judge, filed a concurring opinion.

O'Scannlain, Circuit Judge, filed an opinion concurring in part and dissenting in part.

West Headnotes

[1] Armed Services 34 ⚿3(2)

34 Armed Services
34I In General
34k3 Relation of Military to Civil Authority
34k3(2) k. Posse comitatus. Most Cited Cases

The Posse Comitatus Act (PCA) prohibits Army and Air Force military personnel from participating in civilian law enforcement activities. 18 U.S.C.A. § 1385.

[2] Armed Services 34 ⚿3(2)

34 Armed Services
34I In General
34k3 Relation of Military to Civil Authority
34k3(2) k. Posse comitatus. Most Cited Cases

Although the Posse Comitatus Act (PCA) does not directly reference the Navy, the restriction on military personnel providing direct assistance to civilian law enforcement applies to the Navy, including agents of the Naval Criminal Investigative Service (NCIS), as a matter of Department of Defense (DoD) and Naval policy. 10 U.S.C.A. § 375; 18 U.S.C.A. § 1385; 32 C.F.R. § 182.6(a)(2).

[3] Armed Services 34 ⚿3(2)

34 Armed Services
34I In General
34k3 Relation of Military to Civil Authority
34k3(2) k. Posse comitatus. Most Cited Cases

The regulations and policies implementing the Posse Comitatus Act (PCA) generally prohibit direct military involvement in civilian law enforcement activities but permit indirect assistance such as the transfer of information obtained during the normal course of military operations or other actions that do not subject civilians to the use of military power that is regulatory, prescriptive, or compulsory. 10 U.S.C.A. § 375; 18 U.S.C.A. § 1385.

[4] Armed Services 34 ⚿3(2)

34 Armed Services
34I In General
34k3 Relation of Military to Civil Authority
34k3(2) k. Posse comitatus. Most Cited Cases

Military involvement in civilian law enforcement constitutes permissible indirect assistance under the Posse Comitatus Act (PCA) and implementing regulations if the involvement: (1) does not constitute the exercise of regulatory, proscriptive, or compulsory military power; (2) does not amount to direct active involvement in the execution of the laws; and (3) does not pervade the activities of civilian authorities. 10 U.S.C.A. § 375; 18 U.S.C.A. § 1385.

[5] Armed Services 34 ⚿3(2)

34 Armed Services
34I In General
34k3 Relation of Military to Civil Authority
34k3(2) k. Posse comitatus. Most Cited Cases

The broad investigation of a special agent of the Naval Criminal Investigative Service (NCIS) into the sharing of child pornography violated the regulations and policies proscribing direct military enforcement of civilian laws, where the agent searched for sharing of child pornography by anyone within the state of Washington, not just those on a military base or with a reasonable likelihood of a Navy affiliation, and the agent's investigation was not in support of any civilian law enforcement action. 10 U.S.C.A. § 375; 18 U.S.C.A. § 1385.

[6] Armed Services 34 ⚿3(2)

34 Armed Services
34I In General
34k3 Relation of Military to Civil Authority
34k3(2) k. Posse comitatus. Most Cited Cases

Criminal Law 110 ⚿392.30

110 Criminal Law
110XVII Evidence
110XVII(I) Competency in General
110k392.1 Wrongfully Obtained Evidence
110k392.30 k. Posse comitatus violations. Most Cited Cases

The government's widespread and repeated violation of regulations and policies prohibiting military personnel providing direct assistance to civilian law enforcement warranted application of the exclusionary rule to evidence of child pornography discovered by a special agent of the Naval Criminal Investigative Service (NCIS) and provided to law enforcement, where agents routinely monitored all computers online in Washington state, regardless of a military connection, and the government had been cautioned about such conduct in prior cases. 10 U.S.C.A. § 375; 18 U.S.C.A. § 1385.

***827** Erik B. Levin (argued), Law Office of Erik B. Levin, Berkeley, CA, for Defendant–Appellant.

Marci Ellsworth (argued), Assistant United States Attorney, and Jenny A. Durkan, United States Attorney, Western District of Washington, Seattle, WA, for Plaintiff–Appellee.

Appeal from the United States District Court for the Western District of Washington, Marsha J. Pechman, Chief District Judge, Presiding.

Before: DIARMUID F. O'SCANNLAIN, ANDREW J. KLEINFELD, and MARSHA S. BERZON, Circuit Judges.

Opinion by Judge BERZON.

Concurrence by Judge KLEINFELD.

Partial Concurrence and Partial Dissent by Judge O'SCANNLAIN.

OPINION

BERZON, Circuit Judge:

A special agent of the Naval Criminal Investigative Service (NCIS) launched an investigation for online criminal activity by anyone in the state of Washington, whether connected with the military or not. The agent found evidence of a crime committed by a civilian in the state and turned it over to civilian law enforcement officials. The civilian, Michael **Dreyer**, was prosecuted, convicted, and sentenced to eighteen years in prison. We hold that the NCIS agent's investigation constituted improper military enforcement of civilian laws and that the evidence collected as a result of that investigation should have been suppressed.

BACKGROUND

In late 2010, NCIS Special Agent Steve Logan began investigating the distribution of child pornography online. Several months later, from his office in Georgia, Agent Logan used a software program, RoundUp, to search for any computers located in Washington state sharing known ***828** child pornography on the Gnutella file-sharing network.[FN1]

FN1. **Dreyer** challenges the admission of evidence related to RoundUp, arguing it did not meet the requirements for the admission of expert testimony established by Federal Rule of Evidence 702 and *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579, 113 S.Ct. 2786, 125 L.Ed.2d 469 (1993). Because we conclude that suppression was warranted for other reasons, we do not reach this issue.

Agent Logan found a computer using the Internet Protocol (IP) address 67.160.77.21 sharing several files identified by RoundUp as child pornography.[FN2] He downloaded three of the files, two images and a video, from that computer. After viewing the files, Agent Logan concluded that they were child pornography.

FN2. RoundUp identified such files by comparing the "SHA–1 hash values" of files being offered for download—unique identifiers that do not change when a file name is altered—with values already known to be associated with child pornography.

Thereafter, Agent Logan made a request for an administrative subpoena for the name and address associated at the time of the downloads with the IP address. He submitted his request to NCIS's representative at the National Center for Missing and Exploited Children, which turned the request over to the Federal Bureau of Investigation (FBI). The FBI sent an administrative subpoena to Comcast. Comcast responded by providing **Dreyer's** name and address in Algona, Washington.

After receiving that information, Agent Logan checked a Department of Defense (DoD) database to determine if **Dreyer** had a military affiliation. He found that **Dreyer** had no current military affiliation.[FN3] Agent Logan then wrote a report summarizing his investigation and forwarded it and the supporting material to the NCIS office in the state of Washington. That office then turned the information over to Officer James Schrimpsher of the Algona Police Department.

FN3. **Dreyer** had previously been a member of the Air Force.

Officer Schrimpsher verified that **Dreyer** lived in Algona based on property and utility records. Because Officer Schrimpsher had never worked on any case involving internet crimes or child pornography, he contacted the Internet Crimes Against Children Task Force for assistance and was referred to Detective Ian Polhemus of the Seattle Police Department. Detective Polhemus reviewed some of the information in the NCIS report, and provided Officer Schrimpsher with a sample of a search warrant affidavit.

Subsequently, Officer Schrimpsher sought, and was issued, a search warrant by a state court judge.[FN4] Officer Schrimpsher, along with several other officers, including Detective Polhemus, Detective

Timothy Luckie of the Seattle Police Department, and Sergeant Lee Gaskill of the Algona Police Department, executed the search warrant. At **Dreyer's** residence, Detective Luckie conducted an on-site "preview" search of a desktop computer he found in the house. FN5 He identified ***829** some images as possible child pornography and directed the Algona officers to seize the computer.

> FN4. Officer Schrimpsher prepared the search warrant application. Officer Schrimpsher testified that he attached Agent Logan's report and supporting material to his affidavit. In drafting the affidavit, he copied and pasted large sections of Detective Polhemus's sample. As a result, Officer Schrimpsher made a number of false representations in his affidavit.
>
> **Dreyer** raises a *Franks* issue regarding the falsities in the affidavit. As we hold suppression was required on other grounds, we do not address this issue.
>
> FN5. We do not address **Dreyer's** contention that the on-site search of his computer exceeded the scope of the state warrant, as we conclude that suppression is appropriate for a different reason.

Months later, United States Department of Homeland Security Special Agent Cao Triet Huynh applied for a warrant to search the electronic media seized from **Dreyer's** home. Huynh based his application on the media found by Agent Logan and Detective Luckie, as well as incriminating statements **Dreyer** made during the car ride. A federal magistrate judge issued a search warrant. The resulting forensic examination of **Dreyer's** computer revealed many videos and images of child pornography.

Dreyer was charged with one count of distributing child pornography on April 14, 2011 in violation of 18 U.S.C. §§ 2252(a)(2) and (b)(1), and one count of possessing child pornography on July 6, 2011 in violation of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2). He moved to suppress the evidence seized during the July 6, 2011 search, as well as the evidence found during the later federal search of the computer.

In his reply brief on his suppression motion, **Dreyer** argued that, as an NCIS agent, Agent Logan had no lawful authority to investigate civilian crime. The government filed a surreply addressing that argument. The parties addressed this issue again at the hearing on the motion to suppress. Following an evidentiary hearing, the district court orally denied his motion to suppress.

Subsequently, following a four-day jury trial, **Dreyer** was convicted of both charges and sentenced to 216 months of incarceration and lifetime supervised release. He timely appealed.

DISCUSSION

Dreyer argues that the fruits of the NCIS investigation into his online file sharing should have been suppressed because military enforcement of civilian laws is prohibited. Because the issue of whether the NCIS involvement violated the limitations on military enforcement of civilian laws "is a mixed question of fact and law which is primarily legal," we review de novo the district court's denial of **Dreyer's** motion to suppress based on this claim. *United States v. Hitchcock,* 286 F.3d 1064, 1069 (9th Cir.), *as amended by* 298 F.3d 1021 (9th Cir.2002).

I.

[1] The Posse Comitatus Act (PCA), 18 U.S.C. § 1385, FN6 "prohibits Army and Air Force military personnel from participating in civilian law enforcement activities." *United States v. Chon,* 210 F.3d 990, 993 (9th Cir.2000). FN7 In addition, Congress***830** has directed "[t]he Secretary of Defense [to] prescribe such regulations as may be necessary" to prevent "direct participation by a member of the Army, Navy, Air Force, or Marine Corps" in civilian law enforcement activities unless otherwise authorized by law. 10 U.S.C. § 375. Congress has

authorized certain exceptions to § 375, such as permitting the military to make equipment and facilities available to civilian law enforcement and allowing the military to provide support in particular situations, such as during an emergency situation involving a weapon of mass destruction. *See* 10 U.S.C. §§ 372–74, 379–82. None of these specific exceptions are at issue here.

FN6. The PCA states, "Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both." 18 U.S.C. § 1385.

FN7. "Posse comitatus (literally 'power of the country') was defined at common law as all those over the age of 15 upon whom a sheriff could call for assistance in preventing any type of civil disorder." H.R.Rep. No. 97–71, pt. 2, at 4 (citing 1 William Blackstone, Commentaries 343–44). Although the PCA itself "was enacted during the Reconstruction Period to eliminate the direct active use of Federal troops by civil law authorities" to enforce the civil law, *United States v. Banks*, 539 F.2d 14, 16 (9th Cir.1976); *see also United States v. Red Feather*, 392 F.Supp. 916, 921–25 (D.S.D.1975), it reflected long-standing American concerns about the use of the military to keep the civil peace, *United States v. Walden*, 490 F.2d 372, 375 (4th Cir.1974); *see also* The Declaration of Independence paras. 11, 12, 14 (U.S.1776) (criticizing the King of Great Britain for having "kept among us, in times of peace, Standing Armies without the Consent of our legislatures"; "affected to render the Military independent of and superior to the Civil power"; and "Quartering large bodies of armed troops among us"); 7 Cong. Rec. 3586 (1878) (remarks of Rep. William Kimmel).

We have previously recognized that, "[a]lthough the PCA does not directly reference the Navy," "PCA-like restrictions" apply to the Navy as a matter of Department of Defense (DoD) and Naval policy. *Chon*, 210 F.3d at 993; *see also United States v. Khan*, 35 F.3d 426, 431 (9th Cir.1994). Specifically, DoD policy states that its "guidance on the Posse Comitatus Act ... is applicable to the Department of the Navy and the Marine Corps as a matter of DoD policy, with such exceptions as may be provided by the Secretary of the Navy on a case-by-case basis." DoD Directive (DoDD) 5525.5 Enclosure 4 E4.3 (Jan. 15, 1986). FN8 "[T]he Secretary of the Navy, using nearly identical language, has adopted this policy." *Chon*, 210 F.3d at 993 (citing former Secretary of the Navy Instructions (SECNAVINST) 5820.7B (March 28, 1988)); *see* SECNAVINST 5820.7C (Jan. 26, 2006).

FN8. After Agent Logan's actions at issue in this appeal, on February 27, 2013, DoD issued Instruction No. 3025.21, which incorporated the substance of, and cancelled, Directive No. 5525.5. *See* DoD Instruction (DoDI) 3025.21(1)(c). Like the cancelled Directive, Instruction No. 3025.21 also provides, "By policy, Posse Comitatus Act restrictions (as well as other restrictions in this Instruction) are applicable to the Department of the Navy (including the Marine Corps) with such exceptions as the Secretary of Defense may authorize in advance on a case-by-case basis." DoDI 3025.21, Enclosure 3(3). The other relevant provisions also remain materially unchanged, except as otherwise indicated later in this opinion.

In addition, on April 13, 2013, the Department of Defense issued a final rule promulgating regulations concerning the

> restriction on military support of civilian law enforcement. *See* Defense Support of Civilian Law Enforcement Agencies, 78 Fed.Reg. 21826–02 (codified at 32 C.F.R. § 182 (2013)). The rule was originally proposed on December 28, 2010. 75 Fed.Reg. 81547–01. The regulations as issued are largely identical to the DoD Instruction No. 3025.21.

The government maintains that, even though PCA-like restrictions apply to the Navy, they do not apply to civilian NCIS agents. *Chon* rejected the same argument. There, as here, the government argued that "§ 375 does not apply to the NCIS because most of its agents are civilians," and "it is headed by a civilian director with a civilian chain of command." *Id.* at 993–94. The government based its first argument on provisions in DoD and Naval policies that

> exempt four categories of people from PCA-like restrictions: (1) members of reserve components when not on active duty; (2) members of the National Guard when not in the Federal Service; (3) civilian employees of DoD unless under the direct command and control of a military officer; and (4) military service members when off duty and in a private capacity.

***831** *Id.* at 993. *Chon* interpreted "these exemptions to mean that the PCA and PCA-like restrictions function to proscribe use of the strength and authority of the military rather than use of the private force of the individuals who make up the institution." *Id.* "In other words, while DoD personnel may participate in civilian law enforcement activities in their private capacities, they may not do so under the auspices of the military." *Id.* Applying this understanding, *Chon* held that the PCA-like restrictions do apply to "civilian NCIS agents" who "represented and furthered the interests of the Navy," and were not distinguishable by the civilians who might interact with them from members of the military. *Id.* These same status-based exemptions are maintained in the regulations and policies today. *See* SECNAVINST 5820.7C(8)(e)(1)–(4); DoDD 5525.5, Enclosure 4 E4.2; *see also* 32 C.F.R. § 182.6(a)(2); DoDI 3025.21, Enclosure 3(2). We see no basis for revisiting our prior interpretation of them.

Chon also rejected the government's second contention, "that the NCIS should be exempt from PCA-like restrictions because it is headed by a civilian director with a civilian chain of command." 210 F.3d at 993–94. The court reasoned that "the NCIS Director has a direct reporting relationship to the Chief of the Naval Operations, a military officer," and so "[d]espite a civilian Director, the NCIS continues to be a unit of, and accountable to, the Navy." *Id.* The government argues that *Chon*'s reasoning has been undermined, because the "reporting relationship" between the NCIS director and the Chief of Naval Operations "was eliminated in 2005" when the Secretary of the Navy issued Instruction 5430.107.

The government is incorrect. At the time that *Chon* was decided, the command structure of NCIS was set forth in Instruction 5520.3B, which provided, "The Director, NCIS reports directly to the Secretary of the Navy," and "[i]n addition, the Director, NCIS reports to the Chief of Naval Operations for physical, personnel and information security." SECNAVINST 5520.3B(4). Instruction 5430.107 has since cancelled Instruction 5520.3B, *see* SECNAVINST 5430.107(2) (Dec. 28, 2005), and now provides, "The Director, NCIS reports directly to the Secretary of the Navy," and "[i]n addition, the Director, NCIS serves as Special Assistant for Naval Investigative Matters and Security to the Chief of Naval Operations," SECNAVINST 5430.107(5)(a). That the NCIS director still serves as the "Special Assistant" to the Chief of Naval Operations means a reporting relationship continues to exist. In addition, Instruction 5430.107 created a Board of Directors that oversees NCIS strategy and operations; the Board includes several military officers. *See* SECNAVINST 5430.107(5)(c) (establishing Board of Directors including the Vice

Chief of Naval Operations and the Assistant Commandant of the Marine Corps). So the change in NCIS's policies regarding its command structure did not undermine this portion of *Chon*'s reasoning.

More fundamentally, the government's assertion that there is a meaningful difference between civilian and other employees of the Navy for the purposes of the PCA-like restrictions is unsound. The DoD policies have consistently proclaimed that they set forth "restrictions on participation of DoD personnel in civilian law enforcement activities." *See* DoDD 5525.5, Enclosure 4; DoDI 3025.21, Enclosure 3. They do not limit their reach to non-civilian personnel only. And any contention to the contrary is belied by the abundantly clear expressions in the most recent regulations and policy instructions. Both state that they "[a]ppl[y] to civilian employees of the DoD Components," and that their restrictions***832** on direct participation in civilian law enforcement "apply to all actions of DoD personnel worldwide," with "DoD personnel" defined to include "Federal military officers and enlisted personnel and civilian employees of the Department of Defense." 32 C.F.R. §§ 182.2(e), 182.3, 182.4(c); DoDI 3025.21(2)(e), (4)(c), Glossary Part II.[FN9]

FN9. Although the most recent DoD Instruction and regulations were issued after the search at issue here, their content is largely identical to that contained in the earlier DoD Directive. Also, the Army policy implementing the newer Instruction and regulation is the same one that implemented the earlier Directive. So the DoD's explanations of the intent and meaning of the newer documents is a useful aid into interpreting the earlier ones. *Cf. Pipefitters Local Union No. 562 v. United States*, 407 U.S. 385, 412, 92 S.Ct. 2247, 33 L.Ed.2d 11 (1972).

[2] Accordingly, we re-affirm *Chon*'s holding that NCIS agents are bound by PCA-like restrictions on direct assistance to civilian law enforcement.

II.

[3] The regulations and policies implementing the PCA and § 375 "generally prohibit 'direct' military involvement in civilian law enforcement activities but permit 'indirect' assistance such as the transfer of information obtained during the normal course of military operations or other actions that 'do not subject civilians to [the] use [of] military power that is regulatory, prescriptive, or compulsory.' " *United States v. Hitchcock*, 286 F.3d at 1069 (citations omitted). Prohibited direct assistance includes "[u]se of military personnel for surveillance or pursuit of individuals, or as undercover agents, informants, investigators, or interrogators." DoDD 5525.5, Enclosure 4, E4.1.3.4.

[4] We have "set forth three tests for determining whether military involvement in civilian law enforcement constitutes permissible indirect assistance: '[1] The involvement must not constitute the exercise of regulatory, proscriptive, or compulsory military power, [2] must not amount to direct active involvement in the execution of the laws, and [3] must not pervade the activities of civilian authorities.' " *Hitchcock*, 286 F.3d at 1069 (quoting *Khan*, 35 F.3d at 431).[FN10] "If any one of these tests is met, the assistance is not indirect." *Khan*, 35 F.3d at 431.

FN10. *Khan* interpreted 32 C.F.R. § 213.10, a regulation that has since been withdrawn. *See* 58 Fed.Reg. 25,776 (Apr. 28, 1993). *Hitchcock* recognized that the withdrawn regulation's relevant provisions remained in DoD Directive 5525.5 as it was in effect at the time of the search at issue here. 286 F.3d at 1069–70 n. 8. Those same provisions are maintained in DoD Instruction No. 3025.21 and the new regulations. *See* 32 C.F.R. § 182.6; DoDI 3025.21, Enclosure 3.

[5] Agent Logan's RoundUp surveillance of all computers in Washington amounted to impermissible direct active involvement in civilian enforcement of the child pornography laws, not permiss-

ible indirect assistance. He acted as an investigator, an activity specifically prohibited as direct assistance. DoDD 5525.5, Enclosure 4, E4.1.3.4; *see also Red Feather*, 392 F.Supp. at 925 ("Activities which constitute an active role in direct law enforcement" include "investigation of crime ... and other like activities."). Agent Logan's actions were akin to the conduct that the Fourth Circuit held violated these regulations in *United States v. Walden*, 490 F.2d 372, 373–76 (4th Cir.1974), where Marines engaged in undercover investigations into store employees' illegal firearms sales to minors and to individuals not residents of the state.

***833** Also, Agent Logan engaged in his investigation not in any support capacity to civilian law enforcement, but rather as an independent actor who initiated and carried out this activity. His actions thus were not "incidental" to the overall investigation into **Dreyer**, or limited to backup support. *Cf. Khan*, 35 F.3d at 432; *United States v. Klimavicius–Viloria*, 144 F.3d 1249, 1259 (9th Cir.1998). The results of his investigation served as the primary basis for the state search warrant. Officer Schrimpsher conducted no significant additional investigation before procuring the warrant—he only verified that **Dreyer** lived at the address he was given and that the descriptions that Agent Logan provided of the files seemed to describe child pornography. Without Agent Logan's identification of **Dreyer**, his computer, and the child pornography on his computer, there would have been no search and no prosecution.

Accordingly, Agent Logan's actions amounted to direct assistance to civilian law enforcement. The government nonetheless argues that Agent Logan's investigation was proper because it falls into the "independent military purpose" exception to the prohibition on direct assistance.

The policies and regulations create "an exception to the general prohibition on direct involvement where" there is "an independent military purpose," that is, "where the military participation is undertaken 'for the primary purpose of furthering a military or foreign affairs function of the United States, regardless of incidental benefits to civilian authorities.' " *Hitchcock*, 286 F.3d at 1069 (quoting DoD Directive 5525.5, Enclosure 4, E4.1.2.1). Such military activities include "[i]nvestigations and other actions related to enforcement of the Uniform Code of Military Justice." DoD Directive 5525.5, Enclosure 4, E.4.1.2.1.1.

The Uniform Code of Military Justice prohibits distribution of child pornography by a member of the armed forces. It has assimilated the elements of the federal child pornography statute through Article 134, its general provision that prohibits "all conduct of a nature to bring discredit upon the armed forces." 10 U.S.C. § 934; *see, e.g., United States v. Brown*, 529 F.3d 1260, 1263–64 (10th Cir.2008). In 2011, the President issued Executive Order 13593, adding to the Manual for Courts Martial a specific Article 134 provision for child pornography. Investigation by military law enforcement officers of possession and distribution of child pornography by military personnel is therefore proper.

But Agent Logan's search was not reasonably focused on carrying out such a legitimate military investigation.[FN11] NCIS is authorized to investigate criminal operations that "significantly affect the naval establishment." SECNAVINST 5430.107(3)(c), 7(b)(2). Agent Logan understood that he did not have the authority to search *any* location, but had to limit his searches to areas where there was "a Department of Navy interest." Yet, Agent Logan's search did not meet the required limitation. He surveyed *the entire state of Washington* for computers sharing child pornography. His initial search was not limited to United States military or government computers, and, as the government acknowledged, Agent Logan had no ***834** idea whether the computers searched belonged to someone with any "affiliation with the military at all." Instead, it was his "standard practice to monitor all computers in a geographic area," here, *every* computer in the state of Washington.

FN11. Because Agent Logan's investiga-

> tion itself violated the PCA-like restrictions, it is irrelevant whether it was permissible for him to transfer to civilian authorities "information collected during the normal course of military training or operations that may be relevant to a violation of any Federal or State law within the jurisdiction of such officials." 10 U.S.C. § 371(a); *see also* DoD Directive 5525.5, Enclosure 2, E.2.1, Enclosure 4, E4.1.7.1; SECNAVINST 5820.7C(5); *Hitchcock,* 286 F.3d at 1069.

Agent Logan's further investigation into **Dreyer's** specific computer and identity also was not reasonably limited to searching for crimes that "significantly affect the naval establishment." SECNAVINST 5430.107(3)(c), 7(b)(2). Agent Logan testified that RoundUp displays the geographic location of the IP address "within a 25– to 30–mile radius." The screen shot for Agent Logan's search shows that RoundUp identified the geographic location for **Dreyer's** IP address as Federal Way, Washington. Agent Logan did not report at the evidentiary hearing on the suppression motion or at trial that he chose to pursue that IP address based on this geographic identification.

Agent Logan did write in his administrative subpoena request that the "Suspect IP was identified in area of large DOD and USN saturation indicating likelihood of USN/DOD suspect." But the record contains no evidence establishing any meaningful military "saturation" of the area at issue. Although the government represents that Federal Way, Washington is located within thirty miles of several military installations, it also is similarly near both Seattle and Tacoma, as well as much of the surrounding metropolitan areas.[FN12] The three-thousand-square-mile area circling Federal Way—the approximate area of a circle with a thirty-mile radius—encompasses much of the state's civilian population. That Agent Logan ended his investigation once he confirmed that **Dreyer** had no current military affiliation is of no matter; his overly broad investigation until that point had already exceeded the scope of his authority.

> FN12. We may properly take judicial notice of United States Census Bureau data, as such data "can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned." Fed.R.Evid. 201(b)(2); *see United States v. Esquivel,* 88 F.3d 722, 726–27 (9th Cir.1996); *Skolnick v. Bd. of Comm'rs of Cook Cnty.,* 435 F.2d 361, 363 (7th Cir.1970).
>
> The United States Census Bureau's 2011 population estimate for the Seattle–Tacoma–Bellevue Metropolitan Statistical Area was about 3.5 million. *See* U.S. Census Bureau, Annual Estimates of the Population of Metropolitan and Micropolitan Statistical Areas: April 1, 2010 to July 1, 2012, *available at* http:// www. census. gov/ popest/ data/ metro/ totals/ 2012/. The Census Bureau estimates that the total state population in that year was about 6.8 million people. *See* U.S. Census Bureau, Annual Estimates of the Population for the United States, Regions, States, and Puerto Rico: April 1, 2010 to July 1, 2013, *available at* http:// www. census. gov/ popest/ data/ index. html.
>
> Census Bureau data also undermines any notion that Federal Way contains significantly more military personnel than other parts of the country. In 2011, the Census Bureau estimated that about 0.4% of Federal Way's adult population was employed by the Armed Forces, the same percentage as it estimated for the United States population. *See* U.S. Census Bureau, 2011 American Community Survey.

The government's position that the military

may monitor and search *all* computers in a state even though it has no reason to believe that the computer's owner has a military affiliation would render the PCA's restrictions entirely meaningless. To accept that position would mean that NCIS agents could, for example, routinely stop suspected drunk drivers in downtown Seattle on the off-chance that a driver is a member of the military, and then turn over all information collected about civilians to the Seattle Police Department for prosecution.

The government's position that the military may search the entire civilian population***835** of a state is also inconsistent with a basic principle underlying the PCA and the related statutes and regulations, "a traditional and strong resistance of Americans to any military intrusion into civilian affairs." *Laird v. Tatum*, 408 U.S. 1, 15, 92 S.Ct. 2318, 33 L.Ed.2d 154 (1972). The PCA was originally enacted on the understandings that "[t]he great beauty of our system of government is that it is to be governed by the people," and that if we use the "military power ... to discharge those duties that belong to civil officers and to the citizens," we "have given up the character of [our] Government; it is no longer a government for liberty; it is no longer a government founded in the consent of the people; it has become a government of force." 7 Cong. Rec. 4247 (1878) (remarks of Sen. Benjamin Hill). Consistent with those fundamental premises, DoD policy warns against an expansive reading such as the one espoused by the government here: Directive 5525.5 specifically notes that the independent military purpose exception "must be used with caution, and does not include actions taken for the primary purpose of aiding civilian law enforcement officials or otherwise serving as a subterfuge to avoid the restrictions of" the PCA. DoDD 5525.5, Enclosure 4, E.4.1.2.1.

The lack of any reasonable connection between the military and the crimes that Agent Logan was investigating separates this case from those in which we have applied the independent military purpose exception. In *Hitchcock*, for example, the defendant "sold LSD to Lake, a U.S. Marine, who was, in turn, selling LSD to other military personnel" on his base. 286 F.3d at 1066, 1070. NCIS agents participated in the investigation "in order to determine whether [the defendant] had sold drugs to other military personnel besides Lake." *Id.* at 1070. *Hitchcock* held the independent military purpose exception applicable because the military participation was justified to "determin[e] the extent to which [the defendant's] LSD was being used and distributed on the military base" in violation of the Uniform Code of Military Justice, and to help " 'maintain law and order on a military installation.' " *Id.* (quoting DoDD 5525.5, Enclosure 4, E4.1.2.1.3). And *Chon* applied the exception where NCIS agents were investigating the theft of military equipment from a Naval facility, and so were acting with "the independent military purpose of recovering military equipment." 210 F.3d at 994.[FN13]

> FN13. Similar connections to the military existed in the out-of-circuit cases upon which the government relies. In *Hayes v. Hawes*, 921 F.2d 100, 101–04 (7th Cir.1990), a Navy investigator assisted civilian police investigating drug trafficking in a mall across the street from a Naval base, after a sailor was found with drugs purchased at that mall. And *United States v. Bacon*, 851 F.2d 1312, 1313–14 (11th Cir.1988), found no violation of the PCA where an army investigator assisted civilian law enforcement "to ferret out a source of some of the cocaine being supplied to both civilians and army personnel."

Thus, we hold that Agent Logan's broad investigation into sharing of child pornography by *anyone* within the state of Washington, not just those on a military base or with a reasonable likelihood of a Navy affiliation, violated the regulations and policies proscribing direct military enforcement of civilian laws.

III.

[6] Having held that Agent Logan's investigation violated the restrictions on the use of the military to enforce civilians laws, we consider whether suppression of the resulting evidence should have been ordered here. We have held that "an exclusionary rule should not be applied to violations of 10 U.S.C. §§ 371–378 until a need ***836** to deter future violations is demonstrated." *United States v. Roberts,* 779 F.2d 565, 568 (9th Cir.1986), *superseded by statute on other grounds as recognized in Khan,* 35 F.3d at 432 n. 7. Such a need exists here, as there is evidence of "widespread and repeated violations" of these provisions. *Id.*

The record here demonstrates that Agent Logan and other NCIS agents routinely carry out broad surveillance activities that violate the restrictions on military enforcement of civilian law. Agent Logan testified that it was his standard practice to "monitor[ ] any computer IP address within a specific geographic location," not just those "specific to U.S. military only, or U.S. government computers." He did not try to isolate military service members within a geographic area. He appeared to believe that these overly broad investigations were permissible, because he was a "U.S. federal agent[ ]" and so could investigate violations of *either* the Uniform Code of Military Justice or federal law.

The extraordinary nature of the surveillance here demonstrates a need to deter future violations. So far as we can tell from the record, it has become a routine practice for the Navy to conduct surveillance of all the civilian computers in an entire state to see whether any child pornography can be found on them, and then to turn over the information to civilian law enforcement when no military connection exists. This is squarely a case of the military undertaking the initiative to enforce civilian law against civilians. "There must be an exceptional reason" to invoke the exclusionary rule for violation of posse comitatus-like regulations, *United States v. Harrington,* 681 F.2d 612, 615 (9th Cir.1982), and the broad use of military surveillance of overwhelmingly civilian populations is an exceptional reason.

Agent Logan carried out these searches repeatedly. He was monitoring another computer at the same time that he found **Dreyer's** IP address. And he was involved with at least twenty other child pornography investigations. Further, Agent Logan was not the only NCIS agent who engaged in such searches. He began carrying out these searches with two other agents at least several months before he found **Dreyer's** IP address.[FN14]

> FN14. We note that in *United States v. Holloway,* 531 Fed.Appx. 582 (6th Cir.2013), an NCIS agent also carried out an online child pornography investigation that targeted a civilian. As there is no precedential circuit opinion in *Holloway, see* 6th Cir. R. 32.1(b); *United States v. Utesch,* 596 F.3d 302, 312 (6th Cir.2010), we do not discuss it further.

That a need to deter future violations exists is further supported by the government's litigation positions. The government is arguing vehemently that the military may monitor for criminal activity all the computers anywhere in any state with a military base or installation, regardless of how likely or unlikely the computers are to be associated with a member of the military. Such an expansive reading of the military's role in the enforcement of the civilian laws demonstrates a profound lack of regard for the important limitations on the role of the military in our civilian society.

The existence of these factors make this case unlike those in which courts have declined to require suppression of the evidence resulting from a violation of these laws. In *Roberts,* we concluded that suppression was not necessary because the violation there was not widespread or repeated. 779 F.2d at 568. Similarly, in *United States v. Walden,* 490 F.2d 372, 377 (4th Cir.1974), after holding that the Marines' activities violated the Navy regulations, the Fourth Circuit declined to require suppression, based primarily on "the ***837** fact that this

case is the first instance to our knowledge in which military personnel have been used as the principal investigators of civilian crimes in violation of the Instruction," and so it was unaware of "any other violation, let alone widespread or repeated violations." And in *United States v. Johnson*, 410 F.3d 137, 149 (4th Cir.2005), the court held that exclusion would not be appropriate there because there was no evidence in the record that the conduct complained of occurred frequently or even repeatedly.

In contrast, we have here abundant evidence that the violation at issue has occurred repeatedly and frequently, and that the government believes that its conduct is permissible, despite prior cautions by our court and others that military personnel, including NCIS agents, may not enforce the civilian laws. Accordingly, we find that the district court erred in denying **Dreyer's** motion to suppress. FN15

FN15. We note that, contrary to the government's repeated representations in its brief and at oral argument that "to date, no court has excluded evidence gathered in violation of the Posse Comitatus Act," at least two courts have done so. In *State v. Pattioay*, 78 Hawai'i 455, 896 P.2d 911, 925 (1995), the Hawaii Supreme Court deemed suppression necessary where "to ignore the violation ... would be to justify the illegality and condone the receipt and use of tainted evidence in the courts of this state." And *Taylor v. State*, 645 P.2d 522, 524–25 (Okla.Crim.App.1982), suppressed evidence obtained in violation of the PCA because under the facts of that case, "the illegal conduct by the law enforcement personnel [rose] to an intolerable level as to necessitate an exclusion of the evidence resulting from the tainted arrest."

CONCLUSION

For the reasons set forth above, we reverse the district court's denial of **Dreyer's** motion to suppress, and we remand to the district court for further proceedings consistent with this opinion.

REVERSED AND REMANDED.

KLEINFELD, Senior Circuit Judge, concurring:

I join fully in the majority opinion. I write separately to address applicability of the exclusionary rule to this case. We all agree that the Navy conduct in this case violated the Posse Comitatus policy provisions, though not the criminal Posse Comitatus statute.

Were we suggesting something like application of the exclusionary rule to all Posse Comitatus violations, then application of the exclusionary rule would be inappropriate. And if there were any reason to think that the violation in this case were a fluke, it would be inappropriate. This case, though, amounts to the military acting as a national police force to investigate civilian law violations by civilians.

Generally, the exclusionary rule does not apply to Posse Comitatus violations, in the absence of "widespread and repeated violations" demonstrating a need to deter future violations.[FN1] In this case, unfortunately, that is just what we have. The Navy did not just peek into **Dreyer's** home computer. It peeked into every computer in the State of Washington using the peer-to-peer file sharing program, "Gnutella." That is more "widespread" than any military investigation of civilians in any case that has been brought to our attention. Millions of people use Gnutella, and millions of people live in Washington, so the number of Gnutella users in Washington is likely quite large. As for being "repeated," the Posse Comitatus violation was repeated against every Gnutella user in ***838** Washington. It does not matter that this is the first case we have seen, and that we do not have repeated circuit court cases. The offense is to the people in Washington whose computers were hacked by the Navy, not to this court. The repetition that matters is the repeated invasions of Washingtonians' privacy, as the Navy software went from civilian computer to civilian computer.

FN1. *United States v. Roberts,* 779 F.2d 565, 568 (9th Cir.1986). The same principle applies to violations of the PCA-like regulations that are at issue here.

We have not found another case in this circuit or our sister circuits applying the exclusionary rule to Posse Comitatus violations, but neither have we found another case in which the violations were so massive. The cases deeming the exclusionary rule inapplicable are all quite different factually, as in *Roberts,* where a guided-missile frigate with Coast Guard and Navy personnel aboard caught a drug runner on the high seas. That was one sailboat, not all the computers in the State of Washington using Gnutella. Military surveillance of all the civilian computers in a state is unique, and distinguishable from all the cases we have found that stop short of applying the exclusionary rule.[FN2]

FN2. *Cf. Roberts,* 779 F.2d at 568; *United States v. Walden,* 490 F.2d 372 (4th Cir.1974).

The military not infrequently investigates civilians or assists in civilian law enforcement incidentally to military law enforcement. A Navy shore patrol may break up a fight involving sailors at a waterfront saloon, and turn the civilians over to the local police. The Army may investigate a drug ring on base, and turn civilian spouses living on base and off-base civilian participants over to civilian authorities. There would be little reason to deter military law enforcement in cases like those, and indeed they would ordinarily not even be Posse Comitatus violations.[FN3] This case is different. There could be no bona fide military purpose to this indiscriminate peeking into civilian computers. It should be easy to distinguish this case from run of the mill military law enforcement that incidentally brings about apprehension of civilians.

FN3. *Cf. United States v. Hitchcock,* 286 F.3d 1064 (9th Cir.2002); *United States v. Chon,* 210 F.3d 990, 994 (9th Cir.2000); DoD Directive 5525.5, Enclosure 4, E4.1.2.1.

True, the practical effect of the decision may be to let a criminal go. As Justice Cardozo wrote, application of the exclusionary rule means that "[t]he criminal is to go free because the constable has blundered."[FN4] We are unlikely to see so widespread and repeated a Posse Comitatus violation from the Army or Air Force, because their military personnel would risk prison.[FN5] If the military chooses to become a national police force to detect civilians committing civilian crimes, the Navy would be the branch to use, because the criminal penalty does not apply to Navy personnel. Without the criminal penalty, the exclusionary rule is about all that the judiciary has to deter such widespread and repeated Posse Comitatus violations as we have here. Letting a criminal go free to deter national military investigation of civilians is worth it.

FN4. *People v. DeFore,* 242 N.Y. 13, 21, 150 N.E. 585 (1926).

FN5. *See* 18 U.S.C. § 1385.

O'SCANNLAIN, Circuit Judge, concurring in part and dissenting in part:

Before today, "not a single federal court" had applied the exclusionary rule to violations of the Posse Comitatus Act (PCA), 18 U.S.C. § 1385, and its implementing regulations.[FN1] ***839***United States v. Vick,* 842 F.Supp.2d 891, 894 (E.D.Va.2012). That is no accident. As we have observed, the exclusionary rule is an "extraordinary remedy," *United States v. Roberts,* 779 F.2d 565, 568 (9th Cir.1986), and the Supreme Court has counseled that it is only to be used as a "last resort," *Hudson v. Michigan,* 547 U.S. 586, 591, 126 S.Ct. 2159, 165 L.Ed.2d 56 (2006). Yet, in a breathtaking assertion of judicial power, today's majority invokes this disfavored remedy for the benefit of a convicted child pornographer. It does so without any demonstrated need to deter future violations of the PCA and without any consideration of the "substantial social costs" associated with the exclusionary rule. *United States v. Leon,* 468 U.S.

897, 907, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984). Like my colleagues, I conclude that Agent Logan violated the PCA, and I concur in Parts I and II of the majority opinion. But I respectfully dissent from the majority's misbegotten remedy for that violation.

FN1. To avoid cumbersome constructions, I will not distinguish between the PCA and its implementing regulations, except where it is necessary to do so.

I

The exclusionary rule is "a judicially created remedy of [the Supreme Court's] own making" whose "sole purpose" is "to deter misconduct by law enforcement." *Davis v. United States*, —— U.S. ——, 131 S.Ct. 2419, 2427, 2432, 180 L.Ed.2d 285 (2011) (internal quotation marks omitted). That is a worthy objective, but it "exacts a heavy toll on both the judicial system and society at large." *Id.* at 2427 . Exclusion "undeniably detracts from the truthfinding process and allows many who would otherwise be incarcerated to escape the consequences of their actions." *Pa. Bd. of Prob. & Parole v. Scott*, 524 U.S. 357, 364, 118 S.Ct. 2014, 141 L.Ed.2d 344 (1998). The rule's "bottom-line effect, in many cases, is to suppress the truth and set the criminal loose in the community without punishment." *Davis*, 131 S.Ct. at 2427; *see also Hudson*, 547 U.S. at 591, 126 S.Ct. 2159 (stating that the costs of exclusion "sometimes include setting the guilty free and the dangerous at large").

For these reasons, the Supreme Court has, since the 1970s, "imposed a more rigorous weighing of [the exclusionary rule's] costs and deterrence benefits." *Davis*, 131 S.Ct. at 2427. Gone are the days when courts imposed the exclusionary rule in a manner that was "not nearly so discriminating." *Id.* Under current doctrine, the important and significant costs of the rule "present[ ] a high obstacle for those urging [its] application." *Scott*, 524 U.S. at 364–65, 118 S.Ct. 2014.

In short, exclusion is "our last resort, not our first impulse." *Hudson*, 547 U.S. at 591, 126 S.Ct. 2159.

II

Our precedents reflect this skeptical view of exclusion with regard to violations of the PCA.[FN2] In *United States v. Roberts*, we held that the exclusionary rule should not be applied to evidence obtained as a result of a PCA violation "until a need to deter future violations is demonstrated." 779 F.2d at 568. Such a demonstration requires a showing of "widespread and repeated violations" of the PCA. *Id.*

FN2. Other courts of appeals have recognized that the Supreme Court's description of the exclusionary rule in the Fourth Amendment context applies to PCA cases. *See, e.g., United States v. Al–Talib*, 55 F.3d 923, 930 (4th Cir.1995).

In announcing this rule, we adopted the approach of the Fourth and Fifth Circuits in *United States v. Walden*, 490 F.2d 372, 376–77 (4th Cir.1974), and *United States v. Wolffs*, 594 F.2d 77, 84–85 (5th Cir.1979). Significantly, none of those three cases applied the exclusionary rule to violations of the PCA, and all three referred to the ***840** exclusionary rule as an "extraordinary remedy." *Roberts*, 779 F.2d at 568; *Wolffs*, 594 F.2d at 85; *Walden*, 490 F.2d at 377. Indeed, in *Roberts*, we "consider[ed] it significant that courts have uniformly refused to apply the exclusionary rule to evidence seized in violation of the Posse Comitatus Act." 779 F.2d at 568.

Before today, that description remained true of federal courts.

III

As the foregoing survey of Supreme Court and Ninth Circuit precedent makes clear, the application of the exclusionary rule to violations of the PCA is not automatic. Rather, it is assessed by considering whether "the clear costs of applying an exclusionary rule" are outweighed by "any discernible bene-

fits." *Id.* This case demonstrates that the costs of exclusion substantially outweigh the evanescent benefits. Indeed, it is not a close call.

A

Any evaluation of whether to apply the exclusionary rule to PCA violations must take into account the significant costs of exclusion. In *Walden,* the Fourth Circuit believed that the facts of the case before it were particularly useful in highlighting the costs of exclusion. The Fourth Circuit thought it significant that "the evidence of [the] defendant's guilt [wa]s overwhelming" and that application of the exclusionary rule would have suppressed "the bulk of the evidence" against the defendant. 490 F.2d at 376. The possibility of setting free a convicted felon was a troubling cost of exclusion, and because there was no need to deter future violations, nothing justified incurring such costs. *Id.* at 376–77; *see also United States v. Jones,* 13 F.3d 100, 104 (4th Cir.1993) (recognizing that setting free guilty defendants is a cost courts should consider in determining whether to apply the exclusionary rule to PCA violations).

In **Dreyer's** case, a jury convicted him of possession and distribution of child pornography. As in *Walden,* the evidence of guilt is overwhelming. Using specialized software called RoundUp, Agent Logan searched the state of Washington for computers trafficking in child pornography on the Gnutella file-sharing network. Maj. op. at 827. The software identified a computer bearing the Internet Protocol (IP) address 67.160.77.21 as offering several files of known child pornography to fellow Gnutella users. *Id.* at 827–28. We know that the files contained child pornography because they bear unique identifiers—called "SHA–1 hash values"—that match the identifiers of known child pornography files contained in a database maintained by RoundUp and the National Center for Missing and Exploited Children. *Id.* at 828 The IP address offering child pornography belonged to **Dreyer**. *Id.* Agent Logan, using a method that permitted him to ensure that he was downloading files only from **Dreyer's** computer, downloaded two images and a video, which, upon review, he confirmed contained child pornography. *Id.* Subsequent searches of **Dreyer's** seized hard drives revealed several such files. *Id.* at 828–29. There can be little doubt, then, that **Dreyer** trafficked in child pornography, an activity that is "intrinsically related to the sexual abuse of children." *New York v. Ferber,* 458 U.S. 747, 759, 102 S.Ct. 3348, 73 L.Ed.2d 1113 (1982).

Application of the exclusionary rule would suppress all evidence obtained by Agent Logan. Moreover, as the majority opinion observes, without the evidence obtained by Agent Logan, it is probable that "there would have been no [subsequent] search[es] and no prosecution." Maj. op. at 833. Thus, application of the exclusionary ***841** rule to the allegedly tainted evidence and its fruits is likely to result in a convicted child pornographer being released from prison.

It is impossible to state this conclusion without feeling its gravity. In this context, the Supreme Court's warning against unnecessarily "setting the guilty free and the dangerous at large" should give any jurist pause. *Hudson,* 547 U.S. at 591, 126 S.Ct. 2159. Yet, such a result would not be uncommon if we were to begin applying the exclusionary rule to PCA cases. Thus, the costs of exclusion are high.

B

Despite this cost, application of the exclusionary rule might still be justified if there were evidence of "widespread and repeated violations" of the PCA.[FN3] *Roberts,* 779 F.2d at 568. On this record, there is not.

> FN3. *Roberts* implied that application of the exclusionary rule in the PCA context could be justified, and I do not question that conclusion here. 779 F.2d at 568. However, I note that there is a strong argument to be made that exclusion is *never* justified for violations of the PCA. Several

considerations might support such an argument, such as (1) the fact that Congress could have provided for exclusion had it thought such a remedy was appropriate; (2) the PCA provides for its own enforcement through criminal sanctions, *see* 18 U.S.C. § 1385; and (3) "the [PCA] express[ ] a policy that is for the benefit of the people as a whole, but not one that may fairly be characterized as expressly designed to protect the personal rights of defendants," *Walden*, 490 F.2d at 377. However, even assuming that the exclusionary rule could be applied to the PCA context, I believe we do not yet have a reason to do so.

The majority opinion primarily focuses on Agent Logan's ostensible violations of the relevant regulations applying the PCA to the Navy. Maj. op. at 835–36. But the actions of one agent—no matter how egregious—do not show that violations are widespread. Agent Logan's descriptions of his own practices are, therefore, of limited relevance.

Perhaps recognizing the thinness of this evidence, the majority opinion also points out that Agent Logan "began carrying out these searches with two other agents at least several months before he found **Dreyer's** IP address." *Id.* at 836. It also references another supposed violation in Kentucky. *Id.* at 836 n. 14. I fail to see how evidence that four agents committed violations—three of whom were part of the same investigative team—demonstrates a widespread problem. Such anecdotal evidence falls far short of what our precedents require before we will resort to the "extraordinary remedy" of exclusion, especially considering the cost of doing so in this case. *Roberts*, 779 F.2d at 568. Indeed, at least one of our sister circuits rejected exclusion in the face of similarly scattershot evidence. When the Eleventh Circuit was confronted with five alleged violations of the PCA *within the same circuit* over a ten-year period, it concluded that this amounted to only a "few" incidents that provided "no basis" for applying the exclusionary rule. *United States v. Mendoza–Cecelia*, 963 F.2d 1467, 1478 n. 9 (11th Cir.1992), *abrogated on other grounds as recognized by United States v. Rainey*, 362 F.3d 733, 735 (11th Cir.2004). The argument in favor of exclusion is no more compelling on the record before us.

Finally, the majority opinion cites the government's litigating position in this case as evidence of "a profound lack of regard for the important limitations on the role of the military in our civilian society." Maj. op. at 836. Regardless of whether that observation is true, it does nothing to show that there have, in fact, been widespread and repeated violations of the PCA; ***842** it simply shows that the government wanted to win this case and put forward the best arguments it could to justify what Agent Logan did here. From the premise that the government believes it has a certain power, it does not follow that the government routinely exercises that power. The government's litigating position is, therefore, irrelevant to the *Roberts* inquiry.

Thus, far from having "abundant evidence that the violation at issue has occurred repeatedly and frequently," Maj. op. at 837, we have before us a paucity of evidence that does not come close to overcoming the "high obstacle for those urging application of the [exclusionary] rule." *Scott*, 524 U.S. at 364–65, 118 S.Ct. 2014.

IV

Given the significant costs of exclusion in PCA cases, as well as the meager evidence of PCA violations contained in the record, I would hold that the violation at issue here does not merit application of the exclusionary rule.[FN4] The majority opinion's contrary holding ignores the Supreme Court's clear teaching on exclusion, our own precedents' stringent test for application of that extraordinary remedy, and the uniform rejection of exclusion by federal courts in the PCA context. Because this case provides no justification for setting a convicted child pornographer free, I respectfully dissent.

FN4. As for **Dreyer's** remaining claims, although I would affirm the district court

> across the board, I limit my discussion here to the issue addressed by the majority opinion.

C.A.9 (Wash.),2014.
U.S. v. Dreyer
767 F.3d 826, 14 Cal. Daily Op. Serv. 10,767, 2014 Daily Journal D.A.R. 12,668

END OF DOCUMENT