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