No. 13-30077

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

MICHAEL ALLAN DREYER,

Defendant-Appellant.

On Appeal from United States District Court
Western District of Washington at Seattle
District Court No. CR12-119MJP

The Honorable Marsha J. Pechman
United States District Judge

DEFENDANT-APPELLANT'S OPENING BRIEF

Erik B. Levin
Law Office of Erik B. Levin
1619 Delaware Street
Berkeley, California 94703
Tel. (510) 978-4778
Fax (510) 978-4422

Attorney for Defendant-Appellant
MICHAEL ALLAN DREYER

Table of Contents

Table of Authorities

Cases

Statutes

Other Authorities

Rules

Issues for Review

Four issues are presented in this appeal.

1. The investigation targeting Mr. Dreyer was initiated by the Naval Criminal Investigation Service (NCIS) as part of its larger investigation into Washington state residents trading child pornography over the Gnutella peer-to-peer network. The issue is whether the NCIS investigation violates the prohibition against U.S. military enforcement of civilian laws.

2. The affidavit submitted in support of the search warrant for Mr. Dreyer's home contained multiple misrepresentations and omissions. The issue is whether there was probable cause to search Mr. Dreyer's home once the misrepresentations and omissions had been corrected.

3. During the execution of the search warrant, law enforcement conducted a general search of a computer found within Mr. Dreyer's home despite that fact the warrant only authorized seizure of computers and an offsite search. The issue is whether this search exceeded the scope of the warrant and violated the Fourth Amendment's prohibition against general searches.

4. The final issue is whether this district court violated Federal Rule of Evidence 702 when it denied the defense *Daubert*[1] motion challenging the admissibility of evidence obtained through the RoundUp web-based program, despite the fact that no witness could testify to its reliability.

Relevant Constitutional, Statutory, and Administrative Authority

United States Constitution, Fourth Amendment
The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

[1] *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993).

Posse Comitatus Act, 18 U.S.C. § 1385
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.

10 U.S.C. § 375, Restriction on direct participation by military personnel
The Secretary of Defense shall prescribe such regulations as may be necessary to ensure that any activity (including the provision of any equipment or facility or the assignment or detail of any personnel) under this chapter does not include or permit direct participation by a 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.

Department of Defense Directive 5525.5.
E4.1.3. Restrictions on Direct Assistance. Except as otherwise provided in this enclosure, the prohibition on the use of military personnel "as a posse comitatus or otherwise to execute the laws" prohibits the following forms of direct assistance:

E4.1.3.1. Interdiction of a vehicle, vessel, aircraft, or other similar activity.
E4.1.3.2. A search or seizure.
E4.1.3.3. An arrest, apprehension, stop and frisk, or similar activity.
E4.1.3.4. Use of military personnel for surveillance or pursuit of individuals, or as undercover agents, informants, investigators, or interrogators.

Federal Rules of Evidence 702
A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:

(a) the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;
(b) the testimony is based on sufficient facts or data;
(c) the testimony is the product of reliable principles and methods; and
(d) the expert has reliably applied the principles and methods to the facts of the case.

Statement of Jurisdiction

This appeal is from the judgment rendered by the Honorable Marsha J. Pechman, United States District Judge, on March 15, 2013, sentencing Mr. Michael Allan Dreyer to 216 months' incarceration based on his convictions for distribution of child pornography, in violation of 18 U.S.C. §§ 2252(a)(2) and (b)(1), and possession of child pornography, in violation of 18 U.S.C. §§ 2252(a)(4)(B) and (a)(2). (ER 71; CR 122). The district court had jurisdiction pursuant to 18 U.S.C. § 3231; this Court has jurisdiction pursuant to 28 U.S.C. § 1291.

The judgment was entered March 15, 2013. (ER 70; CR 122). A timely notice of appeal was filed March 22, 2013. (ER 68; CR 125).

Statement of the Case

This appeal is from Mr. Dreyer's conviction following a jury trial. Mr. Dreyer was charged in a two-count indictment on May 3, 2012. (ER 482; CR 11). The allegations in the indictment arose from an undercover investigation by the Naval Criminal Investigative Service into file sharing by Washington state residents over the Gnutella peer-to-peer network on April 14, 2011. (ER 487-8; CR 1). On July 6, 2011, law enforcement executed a search warrant targeting Mr. Dreyer's home. (ER 490; CR 1). During the search of Mr. Dreyer's home, a law enforcement agent searched a desktop computer and discovered several images of

suspected child pornography. (ER 491; CR 1). The District Court denied Mr. Dreyer's motion to suppress the fruits of the search. (ER 60-65; 7/5/12 RT 173-8). Mr. Dreyer proceeded to trial on September 24, 2012, and was convicted of both counts on September 27, 2012. (ER 76; CR 106). On March 14, 2013, the district court sentenced Mr. Dreyer to 216 months' incarceration, lifetime supervised release, and a $200 special assessment fee. (ER 70; CR 122). This appeal followed. (ER 68; CR 125). Mr. Dreyer is currently in the custody of the Bureau of Prisons serving the 216-month sentence imposed in this case.

Statement of the Facts

Naval Criminal Investigation Service Investigation

The investigation of Michael Dreyer began as a U.S. Military investigation into the use of the Gnutella file sharing network by residents of Washington state. (ER 165; 9/24/12 RT 227). NCIS Special Agent Steve Logan, who was stationed in Brunswick, Georgia, began investigating child pornography cases because "we had the opportunity and the equipment and we started that way." (ER 337; 6/22/12 RT 5). The equipment Logan had was a web-based program called RoundUp, with which he conducted his investigations. (ER 338; 6/22/12 RT 6).

RoundUp was created by the Internet Crimes Against Children Training Academy. (*Id.*). According to Logan, RoundUp permits the user to search peer-to-peer networks, such as the Gnutella network. Logan uses RoundUp by specifying a

country and state to be searched and then entering search terms he believes to be indicative of child pornography. (ER 339; 6/22/12 RT 7). Based on these search parameters, RoundUp produces a list of internet protocol addresses[2] that may have child pornography in their shared folder.[3] (ER 339-40; 6/22/12 RT 7-8). RoundUp shows the total number of files in the shared folder as well as the total number of "files of interest," which Agent Logan described as "known image[s] of child pornography." (ER 344; 6/22/12 RT 12).

According to Logan, a known image of child pornography is an image of a victim who has been identified and determined to be under the age of consent at the time the image was created. (ER 128; 9/24/12 RT 190). To determine whether an image is a "known image," RoundUp compares the 16 digit SHA-1 hash value of each image to a database of known images maintained by RoundUp as well as one maintained by the National Center for Missing and Exploited Children. (ER 126-7; 9/24/12 RT 188-9).

Once Logan identifies the files he wants to download, he then "double-click[s] on them and it will give [] a download of that file[.]" (ER 137; 9/24/12 RT

[2] An internet protocol addresses or IP address is “a number provided by the internet service provider, whether it is Comcast, AT&T, or whoever provides internet for your home or business[.]” (ER 341; 6/22/12 RT 9).

[3] Files in the shared folder are available to others on the peer-to-peer file sharing network. (ER 340-1; 6/22/12 RT 8-9).

199). *See also* (ER 350; 6/22/12 RT 18). Logan is not a computer expert and as far he knows there are no test reports, error rates, or validation reports relating to RoundUp. (ER 146-7; 9/24/12 RT 208-9).

On April 14, 2011, Logan began an investigation into Washington state residents trading child pornography over the Gnutella peer-to-peer network after he was contacted by NCIS agents in Washington and asked "to identify individuals trading child pornography in this area." (ER 165, 167; 9/24/12 RT 227, 229). Logan did not limit his search to members or employees of the U.S. military or to computers belonging to the U.S. government. (ER 361; 6/22/12 RT 29). Instead, he set RoundUp to search all computers within Washington state. (ER 147-9; 9/24/12 RT 209-211). Ultimately, Logan downloaded three files of suspected child pornography through RoundUp from an IP address in Washington state. (ER 350-2; 6/22/12 RT 18-20).

Logan then submitted a request to the NCIS representative at the National Center for Missing and Exploited Children seeking an administrative subpoena for the name and address of the internet service subscriber. (ER 352-3; 6/22/12 RT 21-22). In his request for a subpoena, Logan wrote that "Suspect IP was identified in area of large DOD and USN saturation indicating likelihood of USN/DOD suspect." (ER 334; Defense Hearing Exhibit 100). Logan's request was handed off to an FBI agent who submitted the administrative subpoena. (ER 22; 6/22/12 RT

22). The subpoena was returned with Michael Dreyer's name and address in Algona, Washington. (*Id.*).

After determining that Mr. Dreyer had no current military affiliation,[4] Agent Logan prepared a written report which he forwarded to the NCIS Office in Washington state. (ER 356; 6/22/12 RT 24). He had no further involvement in the investigation of Mr. Dreyer and never spoke with anyone at the Algona Police Department. (ER 384; 6/22/12 RT 52).

Agent Logan understood that as an NCIS Agent, he is authorized to conduct criminal investigation relating only to the Department of the Navy, its assets, facilities, and personnel. (ER 337; 6/22/12 RT 5). Logan, nevertheless, testified that he believes that monitoring computers trading in child pornography in the U.S. is an interest of the Navy. (ER 145; 9/24/12 RT 207).

Mr. Dreyer moved to suppress the fruits of the NCIS investigation on several bases, including that it violated the Posse Comitatus Act and related authority. (CR 25 at 6). The Court denied the motion. (ER 64; 7/5/12 RT 177).

Washington State Search Warrant

On May 25, 2011, Algona Police Department Detective James Schrimpsher received a call from NCIS Agent Clergy who was stationed in Washington State

[4] Mr. Dreyer is a retired U.S. Air Force Technical Sergeant. (ER 355; 6/22/12 RT 23).

(ER 387, 410; 6/22/12 RT 55, 78). Clergy informed Schrimpsher about the child pornography investigation targeting Mr. Dreyer. (ER 388-9; 6/22/12 RT 56-57). Schrimpsher verified Dreyer's name and address, but conducted no further investigation on the matter. (ER 388; 6/22/12 RT 56). He received a copy of Agent Logan's report on June 20, 2011, but neither reviewed the evidence, nor spoke with Logan about his investigation. (ER 389, 411; 6/22/12 RT 57, 79). Schrimpsher completed a search warrant application and submitted it to King County District Court on July 5, 2011. (ER 393, 395; 6/22/12 RT 61, 63).

Schrimpsher's search warrant affidavit contained a number of misrepresentations and omissions. In his affidavit, he swore that he personally downloaded the child pornography with special undercover investigative software called E-Phex, on which he had received appropriate training. (ER 281; Government Hearing Exhibit 2). He assured the court that the material he downloaded came directly from Mr. Dreyer's computer. As he wrote in his affidavit, E-Phex "is designed to connect directly to one IP address and browse or download from one specific peer at a time." (*Id.*). This was in contrast to traditional peer-to-peer programs which download from many sources. (*Id.*). According to Schrimpsher, E-Phex "ensures that the files are obtained from the target IP address – assuring a single-source download so that any downloaded file comes directly from the suspect IP address." (ER 283; Government Hearing Exhibit 2). He also

explained to the judge that E-Phex notified him when it had completed the download of the evidence and that it "segregate[d]" the evidence obtained from Mr. Dreyer's computer "from any other evidence." (ER 282; Government Hearing Exhibit 2).

During the evidentiary hearing on Mr. Dreyer's *Franks* hearing, Schrimpsher admitted that none of the information above was true. He did not download anything, had never used (or been trained on) E-Phex, did not know what program Logan utilized in his investigation, and had never heard of RoundUp. (ER 424-8, 444; 6/22/12 RT 92-5, 112). In fact, as Schrimpsher admitted during the hearing, "I have never worked on a child pornography case." (ER 431; 6/22/12 RT 99). As Schrimpsher admitted during the suppression hearing, "I don't have a background in this stuff, I want to know how this stuff kind of works[.]" (*Id.*).

Despite his lack of experience or training, Schrimpsher swore in the search warrant affidavit that based on his "training and experience" possessing and trading child pornography was "need driven behavior" and, as a result, "collections are retained on digital storage media and digital storage media devices long after the image was initially accessed." (ER 284; Government Hearing Exhibit 2).

Schrimpsher made these allegations to support his request to search for and seize a broad array of items including personal computer hardware, computer software applications, computer-related documentation, passwords and security

devices, and digital data. (ER 290; Government Hearing Exhibit 2). The application sought a warrant to search Mr. Dreyer's residence for evidence relating to the possession of child pornography to seize "computer(s) and computer related equipment . . . for searching offsite[.]" (ER 286; Government Hearing Exhibit 2).

Mr. Dreyer moved to suppress the fruits of the warrant under *Franks v. Delaware*, 438 U.S. 154 (1978), arguing that Schrimpsher's reckless and/or intentional material misrepresentations and omissions rendered the search warrant invalid. (CR 18). At the *Franks* hearing, Schrimpsher testified that he was aware of errors in the warrant application and acknowledged that he "should have fixed that." (ER 225; 7/5/12 RT 53). The government conceded that the warrant contained misrepresentations, but argued they were not fatal to the warrant because Schrimpsher appended Logan's report to his affidavit. (ER 3-6; 7/5/12 RT 116-119).

The district court denied the *Franks* motion in a bench order. (ER 60-65; 7/5/12 RT 173-178). The court found that Schrimpsher had made omissions and misrepresentations in the warrant affidavit (particularly in the background section of affidavit), but concluded that even if it were to strike "the background section, and even if the detective had put in that this was his first search warrant, this affidavit is sufficient to support the search that was conducted." (ER 61-2; 7/5/12 RT 174-5).

Schrimpsher's testimony that he attached Logan's report to the search warrant application, (ER 395; 6/22/12 RT 63), was of particular importance to the district court, because Logan's report contained a description of the images as well as Logan's belief they were underage. (ER 61-2; 7/5/12 RT 174-5).

The district court also considered it significant that the court issuing the warrant had the opportunity to question Schrimpsher regarding the source of his information and the veracity of his affidavit. "She had an opportunity to verify what was his work and what was that of Detective Logan's or another officer being relied upon." (ER 62; 7/5/12 RT 175).

Schrimpsher testified that he had explained to the judge who issued the warrant, "the circumstances of how I received the case[.]" (ER 426; 6/22/12 RT 94). According to Schrimpsher, "I explained to her how the information was pulled out[]" and "I did tell her that I was the one that – that the information was obtained from an NCIS agent." (ER 427; 6/22/12 RT 95). He never testified, however, that he revealed his misrepresentations or his omission (regarding his lack of experience) to the judge. (ER 425-7; 6/22/12 RT 93-5).

Search Warrant Execution

Schrimpsher executed the search on July 6, 2011, along with Algona Police Officer Aaron Job and Sergeant Lee Gaskill, Detective David Newton of the

Pacific Police Department and Seattle Police Department Detectives Ian Polhemus and Timothy Luckie. (ER 396; 6/22/12 RT 64).

Soon after arriving at the Dreyer residence, Schrimpsher, Gaskill, and Polhemus left to look for Mr. Dreyer at a local church food bank, where Ms. Dreyer indicated he was a volunteer. (ER 398-9; 6/22/12 RT 66-7). After locating Mr. Dreyer, the officers informed him that he needed to go back to his house with them. (ER 400; 6/22/12 RT 68). On the trip back to Mr. Dreyer's home, Detective Schrimpsher sat in the rear of his vehicle with Mr. Dreyer and digitally recorded his questioning of Mr. Dreyer. (ER 401-4; 6/22/12 RT 69-72). Schrimpsher did not give Mr. Dreyer his *Miranda*[5] warnings and continued to question him even after Dreyer "asked if we could just have a quiet ride." (ER 242; 7/5/12 RT 70). Detective Polhemus testified that prior to detaining Mr. Dreyer, "I explained to Detective Schrimpsher that if it had been my case . . . I would probably advise him [Mr. Dreyer of his *Miranda* rights] because you are technically seizing that person[.]" (ER 244-5; 7/5/12 RT 72-3).

At the conclusion of the suppression hearing, the government "affirmatively indicated that it's not going to seek to use those statements in its case in chief." (ER 10; 7/5/12 RT 123). The government later explained that the "appropriate remedy" for the *Miranda* violation "and one the government has already conceded,

[5] *Miranda v. Arizona*, 384 U.S. 436 (1966).

is that the statements that Mr. Dreyer made, obtained in violation of his Miranda rights, should not and cannot be used in the government's case in chief. We've made that concession." (ER 58; 7/5/12 RT 171).

The district court agreed with the government's concession ruling that the statement "would not see the light of day[.]" (ER 11; 7/5/12 RT 124). In addition to concluding that Mr. Dreyer's *Miranda* rights had been violated, the district court held that his statements were the fruit of an unlawful arrest. (ER 60; 7/5/12 RT 173). As the district court explained, "There is an unlawful arrest. At the time they went to the food bank, they did not have probable cause to arrest him." (ER 63; 7/5/12 RT 176).

Desktop Computer Search

During the search of Mr. Dreyer's home, Detective Timothy Luckie, a forensic examiner with the Internet Crimes against Children Task Force, conducted a forensic search of a desktop computer found in the home. (ER 248, 252; 7/5/12 RT 76, 80). Luckie used a computer forensic tool named TUX4N6 to search the desktop computer. (ER 249-50, 253; 7/5/12 RT 77-78, 81). TUX4N6 permits the user to search "the data stored" on a computer, including "images, movies, text document, and any other data[.]" (ER 250, 253; 7/5/12 RT 78, 81). With the tool, Luckie could "browse the directories, and the folders, and the files" and download that data onto a thumb drive. (ER 251, 255; 7/5/12 RT 79, 83).

Luckie searched the desktop computer for pictures, images, and graphics. (ER 268; 7/5/12 RT 96). As he explained, TUX4N6 "look[s] for file extensions. And it saves all of them. Not anything specific, or notable, or child pornography, or any particular hash value of a child porn picture. It is going strictly by file extension and taking them all, hashing them and then saving them onto the USB thumb drive." (ER 259, 276; 7/5/12 RT 87, 104). *See also* (ER 15; 7/5/12 RT 128**)** (TUX4N6 does not "search[] for a particular type of file name. . . . It's extracting everything with a file extension that's indicative that it's a graphic or a video.")

Using TUX4N6, Luckie previewed the files while downloading them onto the thumb drive. (ER 269; 7/5/12 RT 97). Luckie then reviewed the images captured on the thumb drive to determine if they were possible child pornography. (ER 272; 7/5/12 RT 100). He reviewed a substantial number of files from the computer, perhaps thousands, before identifying approximately six images of suspected child pornography. (ER 258, 273; 7/5/12 RT 86, 101).

The defense argued that the search exceeded the scope of the warrant. (ER 17; 7/5/12 RT 130). "[N]owhere does it say that the officers can, in addition to coming and searching the house and seizing the property, can bring their gear into the house, their computers, and their analysis programs, and begin an on-site analysis at the house, which is exactly what they did." (ER 17-8; 7/5/12 RT 130-1). The district court rejected the argument likening the search of the computer to a

field test for the presence of narcotics. (ER 20; 7/5/12 RT 133). As the district court noted, "some of the computer warrants actually are quite limited as to what it is that they tell people they can do and what kind of teams have to be there when it's done. And this is not limited." (ER 21; 7/5/12 RT 134).

Federal Search Warrant

On December 1, 2011, Department of Homeland Security Special Agent Cao Triet Huynh applied to U.S. Magistrate Judge James P. Donohue for a search warrant of all electronic media seized from Mr. Dreyer's home. (ER 454; Federal Search and Seizure Warrant). Agent Hyunh incorporated the results of Logan's investigation, Schrimpsher's interview of Dreyer (which the district court later suppressed), as well as Luckie's on-site search of the computer found in Mr. Dreyer's home. (ER 462-3, 464-6; Federal Search and Seizure Warrant ¶¶6-9, 14-18). Mr. Dryer moved to suppress the fruit of the federal search warrant. (CR 18). The district court denied the motion. (ER 65; 7/5/12 RT 178).

Summary of the Argument

First, the NCIS investigation into child pornography distribution over the Gnutella peer-to-peer network by residents of Washington state violated the prohibition against use of the military to enforce civilian laws. There was simply no reason to believe the targets of the investigation fell within the jurisdiction of the Navy. The law requires more than the mere possibility that a military interest

could be at stake. Suppression of the fruits of investigation is warranted here to prevent future violations.

Second, the search of Mr. Dreyer's home should be suppressed under *Franks v. Delaware* because the search warrant affidavit was rife with material misrepresentations and omissions. In particular, the search warrant affidavit falsely represented that the affiant had personally downloaded child pornography directly from Mr. Dreyer's computers using specialized software designed to verify the source of contraband. None of this was true.

Moreover, while Schrimpsher met with the judge who issued the warrant, there is no evidence that he corrected his misrepresentations and omissions. Appending Logan's report to the search warrant affidavit did not correct the misrepresentations. In fact, Logan's report contained misrepresentations and omissions of its own.

Third, law enforcement exceeded the scope of the warrant, which authorized the seizure of the computer, and not an onsite search. Despite this, law enforcement conducted a general search of a desktop computer found at Mr. Dreyer's residence in violation of the Fourth Amendment prohibition against general searches.

Finally, the district court abused its discretion when it denied the defense *Daubert* motion and permitted the government to introduce critical evidence

obtained and authenticated through RoundUp without demonstrating that RoundUp was reliable.

Argument

I. The NCIS investigation violated the prohibition against military enforcement of civilian laws.

Standard of Review

Whether the NCIS investigation violated the prohibition on the use of military personnel as a posse comitatus is mixed question of fact and law which is reviewed de novo. *United States v. Hitchcock*, 286 F.3d 1064, 1069 (9th Cir. 2002) (citing *United States v. Roberts*, 779 F.2d 565, 567 (9th Cir.1986)).

A. The Posse Comitatus Act prohibits the military from civilian law enforcement.

The Posse Comitatus Act (PCA), 18 U.S.C. § 1385, prohibits military personnel from participating in civilian law enforcement activities. *United States v. Chon*, 210 F.3d 990, 993 (9th Cir. 2000) (citing 18 U.S.C. § 1385). Congress extended the limitation to all military branches when it instructed the Secretary of Defense to "prescribe such regulations as may be necessary" to prohibit "direct participation by a member of the Army, Navy, Air Force, or Marine Corps in a search, seizure, arrest, or other similar activity" unless otherwise authorized by law. 10 U.S.C. § 375.

In response, the Secretary of Defense issued Directive 5525.5 which generally prohibited all military personnel from providing "direct assistance" to execute civilian laws. *See* Department of Defense Directive 5525.5. at E4.1.3 (Jan 15, 1986, as modified Dec. 20, 1989). The Directive prohibits military personnel from conducting searches and seizures as well as the "surveillance . . . of individuals as undercover agents, informants, investigators, or interrogators." DoD Directive 5525.5 at E4.1.3.2 and E4.1.3.4. The Directive exempted "actions . . . taken for the primary purpose of furthering a military or foreign affairs function of the United States, regardless of incidental benefit to civilian authorities[,]" but warned that the exemption must be "used with caution" and that it does not exempt "actions taken for the primary purpose of aiding civilian law enforcement or otherwise serving as a subterfuge to avoid the restrictions of [the Posse Comitatus Act]." *Id.* at E4.1.2.1.

The Secretary of the Navy placed identical restrictions on direct assistance. *See* SECNAVINST 5820.7C. The Secretary directed that its commands adhere to the Posse Comitatus Act, *see* SECNAVINST 5820.7C at 8.a, and barred its personnel from conducting operations "for the primary purpose of aiding civilian law enforcement officials, or the purpose of routinely collecting information about U.S. citizens." SECNAVINST 5820.7C at 5.b. The restrictions explicitly apply to members of NCIS. *See United States v. Chon*, 210 F.3d 990, 993 (9th Cir. 2000).

B. The NCIS investigation into file sharing by Washington state residents violated the PCA.

NCIS Agent Logan violated the restrictions imposed by the PCA and related authority when he initiated an undercover investigation surveilling file sharing over the Gnutella peer-to-peer network in Washington state and when he caused an administrative subpoena to be issued for subscriber data. Logan's surveillance and search (in the form of an administrative subpoena), are both proscribed by DoD directive and Secretary of the Navy Instruction. *See* Directive 5525.5 at E4.1.3.2 and E4.1.3.4; SECNAVINST 5820.7C at 5.b. Moreover, the investigation was not "taken for the primary purpose of furthering a military or foreign affairs function of the United States[.]" Directive 5525.5 at E4.1.2.1. The Uniform Military Code of Justice applies only to a limited group of individuals with a connection to the military. *See* 10 U.S.C. § 802. Agent Logan had no reason to believe his investigation concerned anyone over whom he had jurisdiction. As the government conceded, Logan had no reason to believe that the people he targeted had any affiliation with the military. (ER 57; 7/5/12 RT 170). His investigation was, first and foremost, a civilian law enforcement investigation.

C. Suppression of the fruit of the investigation is needed to deter future violations.

The Ninth Circuit has held that the exclusionary rule is an appropriate remedy for violations of 10 U.S.C. § 375 when "a need to deter future violations is

demonstrated." *United States v. Roberts*, 779 F.2d 565, 568 (9th Cir. 1986). In this case, the record establishes there is a need to stem future abuses and therefore exclusion is an appropriate remedy.

First, Agent Logan's investigation is not a one-off. As he testified, he routinely investigates child pornography because he has the equipment, namely RoundUp, a web-based computer program. (ER 336-8; 6/22/12 RT 4-6). According to Logan, it is his standard practice "to monitor all computers in a geographic area." (ER 361; 6/22/12 RT 29). He also appears to believe that he has the authority to investigate child pornography regardless of the status of investigation target because "[p]ossession and distribution of child pornography across the internet is a federal crime and we are credentialed U.S. federal agents." (ER 113; 9/24/12 RT 175). According to Logan, the U.S. Navy has an interest in enforcing child pornography laws across the United States. As he testified, "[m]onitoring computers that are trading child pornography in the United States, there are areas of interest of the Department of Navy[.]" (ER 145; 9/24/12 RT 207). The NCIS has been engaging in civilian child pornography investigations as far back as 2008. *See, e.g., United States v. Holloway*, 2011 WL 304580 (W.D.Ky. Jan 27, 2011).

Importantly, unlike other military investigations that merely ended up concerning the enforcement of civilian laws[6], Logan's investigation began by focusing on the public at large on the off chance that it may end up involving individuals over whom the NCIS had jurisdiction. If this type of investigation does not violate the posse comitatus limitation, then nothing will and the exception will have swallowed the rule, something the DoD Directive specifically cautioned against. *See* Directive 5525.5 at E4.1.2.1. For these reasons, the Court should suppress the evidence obtained as a result of the NCIS investigation.

II. The search of Mr. Dreyer's home should be suppressed under *Franks v. Delaware* because of material misrepresentations and omissions in the search warrant affidavit.

Standard of Review

The district court's findings regarding omissions and misrepresentations in affidavits supporting a search warrant are reviewed for clear error. *United States v. DeLeon*, 979 F.2d 761, 763 (9th Cir. 1992) (citing *United States v. Dozier*, 844 F.2d 701, 705 (9th Cir. 1988)). Whether probable cause is lacking because of

---

[6] *See, e.g., United States v. Chon*, 210 F.3d 990, 994 (9th Cir. 2000) (there was an independent military purpose for their investigation the protection of military equipment); *Applewhite v. United States Air Force*, 995 F.2d 997, 1001 (10th Cir.1993) (holding that the military may investigate illegal drug transactions by active duty military personnel); *United States v. Banks*, 539 F.2d 14, 16 (9th Cir.1976) (allowing military personnel to act upon on-base violations of civil law committed by civilians); *United States v. Thompson*, 30 M.J. 570, 574 (1990) (allowing military jurisdiction over a military member who stole both civilian and military property).

misstatements and omissions in the affidavit is reviewed de novo. *See United States v. Elliott*, 322 F.3d 710, 714 (9th Cir. 2003).

A. The Fourth Amendment prohibits warrants containing material misrepresentations and omissions.

In *Franks v. Delaware*, 438 U.S. 154 (1978), the Supreme Court held that if a defendant demonstrates that a facially valid affidavit relies on intentionally or recklessly false statements the evidence obtained on the basis of that search warrant must be excluded. This Court extended *Franks* to omissions of material facts when it held that "the Fourth Amendment mandates that a defendant be permitted to challenge a warrant affidavit valid on its face when it contains deliberate or reckless omissions of facts that tend to mislead." *United States v. Stanert*, 762 F.2d 775, 781 (9th Cir.), *amended*, 769 F.2d 1410 (9th Cir. 1985). "A deliberate or reckless omission by a government official who is not the affiant can be the basis for a *Franks* suppression." *Id.* at 764.

B. The search warrant affidavit contained numerous material misrepresentations and omissions.

There is no dispute that Schrimpsher made substantial misrepresentations in his search warrant affidavit. The government agrees that the warrant contained misrepresentations. *See* (ER 4; 7/5/12 RT 117) ("every time Detective Schrimpsher's affidavit says 'Your affiant did those things,' that's clearly not true").

Even Schrimpsher agreed that the warrant contained misrepresentations, as he testified "I goofed up. I should have fixed that." (ER 225; 7/5/12 RT 53). The district court concluded as much in its bench order. (ER 61-2; 7/5/12 RT 174-5).

Schrimpsher's affidavit assured the judge that she could rely on his representation that the illicit video and two pictures obtained during the investigation came from a computer within Mr. Dreyer's residence. He swore that he had conducted the investigation and personally downloaded the child pornography directly from Mr. Dreyer's computers using specialized software (called E-Phex) designed to verify the source of the contraband. (ER 281-3; Government Hearing Exhibit 2). None of this was true.

Schrimpsher did not do the download, had never used E-Phex, did not know what program Logan utilized in his investigation and had never heard of RoundUp. (ER 424, 444; 6/22/12 RT 92-5, 112). In truth, the only investigative step Schrimpsher took was to verify Mr. Dreyer's address. (ER 388; 6/22/12 RT 56).

Schrimpsher's affidavit also sought broad authority to seize a broad array of items including personal computer hardware, computer software applications, computer-related documentation, passwords and security devices, and digital data. (ER 290; Government Hearing Exhibit 2). Though he had "never worked on a child pornography case[,]" (ER 431; 6/22/12 RT 99), Schrimpsher represented himself as an expert on child pornography and informed the judge that based on his

"training and experience" he knew that possessing and trading child pornography was "need driven behavior" and that "collections are retained on digital storage media and digital storage media devices long after the image was initially accessed." (ER 284; Government Hearing Exhibit 2). At the suppression hearing, however, Schrimpsher admitted "I don't have a background in this stuff, I want to know how this stuff kind of works[.]" (ER 431; 6/22/12 RT 99).

Although the government argued that Schrimpsher's misrepresentations were not intentional, (ER 3; 7/5/12 RT 116), recklessness is sufficient. Moreover, Schrimpsher's history as a law enforcement officer reveals a pattern of dishonesty. This was not Schrimpsher's first instance of making misrepresentations in the course of his employment as a law enforcement officer. He had been fired from the King County Sheriff's Department in 2007 for violating an honesty policy. (ER 207-8, 219; 7/5/12 RT 35-36, 47). The termination came as a result of an internal investigation into three separate arrests by Schrimpsher. (ER 209; 7/5/12 RT 37). During the internal investigation that followed, the King County Sheriff found that Schrimpsher made misleading and intentionally vague statements. (ER 213; 7/5/12 RT 41). His termination was upheld by an arbitrator who concluded that "the King County Sheriff's Office had just cause to discharge [] Schrimpsher for dishonesty during an [Internal Investigation Unit] interview." (ER 212-3; 7/5/12 RT 40-1).

C. The misrepresentations and omissions were material.

The district court denied the *Franks* motion in a bench order. (ER 60-5; 7/5/12 RT 173-178). The court found that Schrimpsher had made misrepresentations in the warrant affidavit (particularly in the background section of affidavit), but concluded that even if it were to strike "the background section, and even if the detective had put in that this was his first search warrant, this affidavit is sufficient to support the search that was conducted. " (ER 61-2; 7/5/12 RT 174-5). Of particular importance to the district court was that Schrimpsher had attached Logan's report to his affidavit, which included a description of the images as well as Logan's conclusion that the subjects were underage. (ER 61-2; 7/5/12 RT 174-5).

Logan's report, however, failed to correct the misrepresentations Schrimpsher made in his affidavit, and, in fact, contained additional misrepresentations. For example, Logan reported that he downloaded three files containing child pornography *directly* from an IP address later determined to belong to Mr. Dreyer. *See* (ER 298; Government Hearing Exhibit 2) ("UCA [Undercover Agent] was able to download three (3) files directly from IP address 67.160.77.21."). During the suppression hearing, Logan clarified that he was actually connected to the IP address through the web-based software RoundUp and

that he downloaded the three files through RoundUp. (ER 349-50; 6/22/12 RT 17-18).

Nor did Logan indicate that he was able to isolate the source of the download. As Schrimpsher revealed in his warrant affidavit, file sharing programs generally "download from many sources" while the forensic program Schrimpsher (falsely) claimed that he used, E-Phex "will only download files from a single source." (ER 281; Government Hearing Exhibit 2). *See United States v. Chiaradio*, 684 F.3d 265, 271 (1st Cir. 2012) (noting that "when a user of the commercially available version of LimeWire tries to download a file, the program seeks out all the users who are sharing the same file and downloads different pieces of that file from multiple locations in order to optimize download speed."). Absent from Logan's report or Schrimpsher's affidavit is any assurance that, like E-Phex, RoundUp is able to isolate downloads from a single source.

Nor is it clear that Logan could have truthfully represented RoundUp capabilities. He testified that he is not computer expert and as far he knows there are no test reports, error rates, or validation reports relating to RoundUp. (ER 146-7; 9/24/12 RT 208-9). *See also* (ER 380-1; 6/22/12 RT 48-49) (Logan testifies that he is unaware of RoundUp's reliability or whether its reliability has been assessed).

Logan's misrepresentation and omission are fatal to the probable cause determination because verifying the source of the download is an indispensable

component of demonstrating probable cause to search Dreyer's computer. To obtain a lawful search warrant, the affiant must demonstrate "probable cause to believe that the legitimate object of a search is located in a particular place." *United States v. Adjani*, 452 F.3d 1140, 1145 (9th Cir. 2006) (quoting *Steagald v.United States*, 451 U.S. 204, 213(1981)). *See United States v. Fernandez*, 388 F.3d 1199, 1252 (9th Cir. 2004) ("Probable cause exists when, considering the totality of the circumstances, the affidavit shows that there is a fair probability that contraband or evidence of a crime will be found in a particular place.") (internal quotation marks and citation omitted).

Without any authentication that illicit files were received from the particular IP address registered to Mr. Dreyer, there is simply no reason to believe that evidence of that crime will be found in his home, particularly since, as noted above, file sharing programs generally download from multiple sources.

Finally, contrary to the district court's conclusion, (ER 62; 7/5/12 RT 175), the fact the issuing court had the *opportunity* to "verify" with Schrimpsher "what was his work and what was that of Detective Logan" does not alter the *Franks* analysis because Schrimpsher failed to correct his misrepresentations. (ER 427; 6/22/12 RT 95). Instead, according to Schrimpsher, he only explained to the judge "the circumstances of how I received the case . . . . how the information was pulled

out . . . [and] that the information was obtained from an NCIS agent." (ER426-7; 6/22/12 RT 94-5).

D. The results of the federal search warrant must also be suppressed as a fruit of the state search warrant.

The federal search warrant relied extensively on the unlawful fruits of the state search warrant and therefore its fruits must be suppressed as well. Agent Hyunh relied on the results of Logan's investigation as well as Luckie's on-site search of the computer found in Mr. Dreyer's home to demonstrate probable cause for the search. (ER 462-3, 464-6; Federal Search and Seizure Warrant ¶¶6-9, 14-18).

Huynh also relied on the illegally-obtained statement and physical evidence taken from Mr. Dreyer to support probable cause. In particular, paragraph 14 of the Hyunh's affidavit highlighted items seized from Mr. Dreyer's automobile following his unlawful arrest. (ER 464; Federal Search and Seizure Warrant ¶14). And paragraph 15 highlighted the admissions Mr. Dreyer's made during his unlawful post-arrest interrogation. (ER 464-5; Federal Search and Seizure Warrant ¶15). When an affidavit contains evidence illegally obtained, "[a] reviewing court should excise the tainted evidence and determine whether the remaining, untainted evidence would provide a neutral magistrate with probable cause to issue a

warrant." *United States v. Vasey*, 834 F.2d 782, 788 (9th Cir. 1987); *United States v. Barajas-Avalos*, 377 F.3d 1040, 1054-1055 (9th Cir. 2004).

Without the information above, the federal warrant lacked probable cause to support the search of the electronic media seized from Mr. Dreyer's home, and its fruit must be suppressed.

III. The fruits of the search should be suppressed because it exceeded the scope of the warrant and was tantamount to a general search in violation of the Fourth Amendment.

Standard of Review

A district court order denying a motion to suppress is reviewed de novo. *United States v. Maddow*, 614 F.3d 1046, 1048 (9th Cir. 2010). Whether a search exceeds the scope of a search warrant is a question of law reviewed de novo. *See United States v. Hurd*, 499 F.3d 963, 965 (9th Cir. 2007).

A. The Fourth Amendment prohibits general searches.

The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures[.]" "The general touchstone of reasonableness which governs Fourth Amendment analysis. . . governs the method of execution of the warrant." *United States v. Ramirez*, 523 U.S. 65, 71 (1998). The reasonableness of a search and seizure depends, in part, on the extent and duration of law enforcement intrusion on personal property and privacy, regardless of whether the initial seizure is lawful.

Winston v. Lee, 470 U.S. 753, 763-66 (1985); *United States v. Place*, 462 U.S. 696, 703 (1983); *see also Kentucky v. King*, 131 S. Ct. 1849 (2011) ("a warrant may not be issued unless probable cause is established *and* the scope of the authorized search is set out with particularity") (emphasis added).

The Fourth Amendment prohibits general warrants. *Andresen v. Maryland*, 427 U.S. 463, 480 (1976). "The Fourth Amendment was a response to the English Crown's use of general warrants, which often allowed royal officials to search and seize whatever and whomever they pleased while investigating crimes." *Ashcroft v. al-Kidd*, 131 S. Ct. 2074, 2084 (2011).

"'Specificity has two aspects: particularity and breadth.'" *United States v. Hill*, 459 F.3d 966, 973 (9th Cir. 2006) (quoting *United States v. Towne*, 997 F.2d 537, 544 (9th Cir. 1993)). "'Particularity is the requirement that the warrant must clearly state what is sought,'" and "'[b]readth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based.'" *Id*. Specificity is intended to prevent the issuance of general warrants, *Marron v. United States*, 275 U.S. 192, 196 (1927), as well as "exploratory rummaging in a person's belongings" even if a warrant has issued. *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971).

United States v. Tamura, 694 F.2d 591 (9th Cir. 1982), is an example of how the manner of execution of an otherwise valid search warrant can violate the

prohibition against general warrants. In *Tamaru*, the FBI executed a warrant which authorized the seizure of certain contract and payment records related to a bribery investigation. During the search, the FBI seized a large quantity of documents and removed them to another location for sorting. 694 F.2d at 595. It was undisputed that relevant and not readily identifiable records were intermingled with the documents that the FBI had taken. Nevertheless, this Court did not approve of "the wholesale seizure for later detailed examination of records not described in the warrant" absent reasonable restrictions on the how the records were handled. *Id.*

The *Tamaru* Court laid down general ground rules the government must follow in cases "where documents are so intermingled that they cannot feasibly be sorted on site[.]" *Id.* These included sealing intermingled records until procedures for segregating evidentiary from non-evidentiary items were approved and monitored by a neutral magistrate. *Id.* at 596. As the Court later explained, "[t]he process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect." *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1117 (9th Cir. 2010) (*CDT III*).

In *United States v. Comprehensive Drug Testing*, 579 F.3d 989 (9th Cir. 2009) (*CDT II*), *opinion revised and superseded by CDT* III, 621 F.3d 1162, this Court mandated several procedural safeguards that must be included in search

warrants for computers and other electronic storage media to ensure that the searches do not become "general search[es]." *Id*. at 998. The first of these safeguards was a requirement that "the government waive reliance upon the plain view doctrine in digital evidence cases." *Id.* at 1006. Second, the Court directed that the government segregate evidentiary and non-evidentiary data, using specialized computer personnel who are not directly involved in the investigation or an "independent third party." *Id*. at 1006. The Court also required the government to provide a detailed "search protocol" that would explain how evidentiary data would be identified and disclosed to investigators; a procedure for returning non-responsive data in a timely manner; and various notices and disclosures to the issuing court. *Id.* The Court concluded by reaffirming that magistrate judges retained discretion to fashion appropriate limits on computer searches and by noting that "[n]othing we could say would substitute for the sound judgment that judicial officers must exercise in striking this delicate balance." *Id*. at 1008.

In formulating these guidelines, this Court largely relied on *Tamura*. *CDT II*, 579 F.3d at 995; *see also id.* at 1006-07. In applying *Tamura* to "the daunting realities of electronic searches," the Court in *CDT II* found that *Tamura* was still good law and "might well have sufficed in this case had its teachings been followed." *CDT II*, 579 F.3d at 1006.

In response to a petition for rehearing by the whole court, the en banc panel issued a revised opinion. *CDT III*, 621 F.3d 1162. The major difference between the two decisions is that the five point summary of search "guidance" contained in the original en banc opinion was moved to a concurring opinion. In all other material respects, the opinions are the same. This includes the Court's rejection of the plain view doctrine in the context of data searches, because it is inconsistent with the requirements of *Tamura*, *see* 621 F.3d at 1170-71; its disapproval of the Government's "deliberate overreaching" in seizing electronic data, *id*. at 1172; and the requirement that judges exercise "greater vigilance" in reviewing searches for electronically stored information. *Id*. at 1177. The Court concluded its revised opinion by renewing its earlier warning that "[t]he process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect." *Id*.

B. The search of the desktop computer found in Mr. Dreyer's home exceeded the scope of the warrant and was tantamount to a general search.

The Court should suppress the fruits of the search warrant because the search of the computer found in Mr. Dreyer's home exceeded the scope of the warrant and was, in effect, a general search in violation of the Fourth Amendment and this Court's *Tamaru* and *CDT III* decisions which require that steps be taken

"to maintain the privacy of materials that are intermingled with seizable materials, and to avoid turning a limited search for particular information into a general search of . . . file systems and computer databases." *CDT III*, 621 F.3d at 1170.

The warrant identified, with particularity, Mr. Dreyer's address as the location to be searched. (ER 286; Government Hearing Exhibit 2). The warrant also provided that "[i]f there is a computer(s) or computer related equipment found we request permission to remove those items as instrumentalities." (*Id.*). The warrant also sought permissions to search them "offsite[.]" *Id. See also* (ER 290; Government Hearing Exhibit 2) ("I am requesting permission to search for, seize, and subsequently examine . . . [p]ersonal computer hardware[.]")

Instead of searching within the scope of the warrant, Detective Luckie testified that he conducted an onsite general search of the desktop computer found in Mr. Dreyer's home. According to Luckie, he used a forensic tool named TUX4N6 to search the desktop computer in Mr. Dreyer's home for pictures, images, and graphics. (ER 268; 7/5/12 RT 96). TUX4N6 "look[s] for file extensions. And it saves all of them. Not anything specific, or notable, or child pornography, or any particular hash value of a child porn picture. It is going strictly by file extension and taking them all, hashing them and then saving them onto the USB thumb drive." (ER 259, 276; 7/5/12 RT 87, 104). During his search, Luckie reviewed a substantial number of files from the computer, perhaps

thousands, before identifying approximately six images of suspected child pornography. (ER258, 273; 7/5/12 RT 86, 101).

The defense argued at the close of the suppression hearing that Luckie's search exceeded the scope of the warrant. (ER 17; 7/5/12 RT 130). "[N]owhere does it say that the officers can, in addition to coming and searching the house and seizing the property, can bring their gear into the house, their computers, and their analysis programs, and begin an on-site analysis at the house, which is exactly what they did." (ER17-8; 7/5/12 RT 130-1). The district court rejected the argument likening the search of the computer to a field test for the presence of narcotics. (ER 20; 7/5/12 RT 133). As the district court noted, "some of the computer warrants actually are quite limited as to what it is that they tell people they can do and what kind of teams have to be there when it's done. And this is not limited." ER 21; 7/5/12 RT134).

The district court missed the point. The search exceeded the scope of the warrant because the warrant did not authorize a search of the computer within Mr. Dreyer's home. Moreover, Luckie's search of the desktop computer was far more than a field test. The search Luckie executed did not follow any of the protocols for the search of electronically stored information suggested by the concurring opinion in *CDT III*. Instead, he examined a broad array of files, despite the fact that the warrant authorized only the seizure of the electronic media for a later search. As a

result, the search exceeded the scope of the warrant, and, in effect, amounted to a general search in violation of the Fourth Amendment. For these reasons, the Court should reverse the district court and suppress the fruits of the search.

IV. The district court abused its discretion when it permitted the government to introduce evidence obtained through and authenticated by the RoundUp program.

Standard of Review

Where, as here, the objection to the admission of evidence has been preserved by filing a motion in limine, *see United States v. Varela-Rivera*, 279 F.3d 1174 (9th Cir. 2002), the district court's decision to admit expert evidence is reviewed for an abuse of discretion and will be reversed only if manifestly erroneous. *United States v. Alatorre*, 222 F.3d 1098, 1100 (9th Cir. 2000). *United States v. Gonzales*, 307 F.3d 906, 909 (9th Cir. 2002).

A. FRE 702 and *Daubert* require the trial court to serve as the gatekeeper of technical and other specialized knowledge.

In *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993), the Supreme Court held that Federal Rules of Evidence "assign to the trial judge the task of ensuring that an expert's testimony both rests on a reliable foundation and is relevant to the task at hand." *Id.* at 597. In particular, "the trial judge *must* determine at the outset, pursuant to Rule 104(a), whether the expert is proposing to

testify to (1) scientific knowledge that (2) will assist the trier of fact to understand or determine a fact in issue." *Id.* at 592 (emphasis added).

Included in this analysis, is "whether the reasoning or methodology underlying the testimony is scientifically valid and . . . whether that reasoning or methodology properly can be applied to the facts in issue." *Id.* at 592-3. While *Daubert* was limited to the context of scientific evidence, *id*. at 590, n.8, the Court later extended its holding "to testimony based on 'technical' and 'other specialized' knowledge." *Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 141 (1999) (quoting Fed. R. Evid. 702). As the proponent of the evidence, the government bears the burden of establishing that the pertinent admissibility requirements are met by a preponderance of the evidence. *See Bourjaily v. United States*, 483 U.S. 171, 175 (1987).

Daubert set forth a non-exclusive checklist for trial courts to use in assessing the reliability of testimony including: (1) whether the expert's technique or theory can be or has been tested–that is, whether the expert's theory can be challenged in some objective sense, or whether it is instead simply a subjective, conclusory approach that cannot reasonably be assessed for reliability; (2) whether the technique or theory has been subject to peer review and publication; (3) the known or potential rate of error of the technique or theory when applied; (4) the existence and maintenance of standards and controls; and (5) whether the technique or theory

has been generally accepted in the scientific community. 509 U.S. at 592-4. *Kumho* held that these factors could be applicable in assessing the reliability of non-scientific expert testimony, depending upon "the particular circumstances of the particular case at issue." *Kumho*, 526 U.S. at 150. Courts have applied *Daubert* to determine whether computer programs, similar to RoundUp, are sufficiently reliable to be proffered as evidence at trial. *See, e.g.*, *United States v. Chiaradio,* 684 F.3d at 276-8.

One thing is clear: the trial court's gatekeeping function requires more than simply "taking the expert's word for it." *See Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 43 F.3d 1311, 1319 (9th Cir. 1995) ("We've been presented with only the experts' qualifications, their conclusions and their assurances of reliability. Under *Daubert*, that's not enough.").

In this case, the district court did just that, it simply took the government's word for it. It also misunderstood the significance RoundUp played in the government's case against Mr. Dreyer and the related need to determine whether its results were reliable. In particular, the district court did not understand that RoundUp not only identified "known child pornography" but that the download Logan conducted utilizing RoundUp was the actus reus underlying the distribution count.

B. The district court erroneously denied the *Daubert* motion because it misunderstood the significance of RoundUp in the government's case against Mr. Dreyer.

Mr. Dreyer moved, pursuant to Fed. R. Evid. 702 and *Daubert*, to preclude electronic evidence obtained through the RoundUp program. (CR 68). In his motion, he argued that the reliability and accuracy of RoundUp was critical, particularly with respect to Count I, distributing child pornography, 18 U.S.C. § 2252(a)(2) and (b)(1), because the government based this count exclusively on evidence obtained and validated through RoundUp. CR 68 at 2.

The district court denied the motion after concluding that RoundUp need not be accurate in order to be admissible. As the district court saw it, RoundUp "is simply a tool for investigation. But the accuracy of the tool is verified by if you find something. In other words, I don't know that the tool has to be accurate all the time if, in fact, at least once it produces what you're looking for." (ER 66; 9/17/12 RT 31). The district court found that since the subsequent search of Mr. Dreyer's computer revealed some evidence of child pornography, RoundUp's reliability could not be challenged. As the Court concluded "it strikes me somewhat like if you're looking for a body you might use a bulldozer or might use a spade, it doesn't really matter. What matters is, did you find the body? So it's somewhat analogous to that, that I don't know that its accuracy really needs to be tested if, in fact, you find something." (*Id.*).

The district court was wrong. RoundUp's reliability and accuracy were critical to the government's proof of the possession and indispensable to its proof of the distribution count.

With respect to the possession count, RoundUp provided evidence that Mr. Dreyer possessed "known child pornography" that RoundUp identified and validated through an comparison to its database. The government introduced a screen shot of the RoundUp program from Logan's April 14, 2011 investigation. (ER 125-6; 9/24/12 RT 181-2); (ER 479; Government Trial Exhibit 100). Logan testified that RoundUp is able to download the SHA-1 value[7] for each image its encounters and then compare that to against its own database, as well as a database at the National Center for Missing and Exploited Children. (ER 126-7; 9/24/12 RT 188-9). Based on this analysis, Logan testified, RoundUp can determine whether the image is a "known image of child pornography." (ER 127; 9/24/12 RT 189). *See also* (ER156-7; 9/24/12 RT 218-9) ("that was confirmed to be child pornography."). If RoundUp determines that the image is a "known image of child pornography" it highlights the file in red and marks it a "file of interest." (ER 132; 9/24/12 RT 194). Utilizing RoundUp, the government concluded that a computer at

[7] Logan testified that the SHA-1number is "a mathematical hash algorithm that is an alphanumeric character that is essentially the digital fingerprint for a particular image or video." (ER 125-6; 9/24/12 RT 187-8).

Mr. Dreyer's IP address contained 11 files of known child pornography. (ER 479; Government Trial Exhibit 100). Only one of those files was shown to the jury. (ER 137; 9/24/12 RT 199).[8]

RoundUp also played an indispensable role in the government's proof of the distribution count. Logan testified that utilizing RoundUp, he downloaded three files which RoundUp identified as "files of interest." (ER 134-7, 150; 9/24/12 RT 196-9, 212). The government based the distribution count exclusively on those files. *See* (ER 487-8; CR 1 ¶4); (ER 482; CR 11 at 1). In other words, RoundUp was an integral part of the actus reus of the distribution count, a point emphasized by the government in summation when it referred to the video Logan downloaded utilizing RoundUp as "the video in connection with the distribution" (ER 79; 9/26/12 RT 141).[9]

Although RoundUp played a critical role in the government's case against Mr. Dreyer, little was known about how it functioned, and thus there was no credible reason to believe that RoundUp functioned any differently than traditional

[8] The government introduced one movie Logan purportedly downloaded as Exhibit 105 and 105-A. (*Id.*).

[9] The government did not refer to the video "in connection with the distribution" by exhibit number, but rather referred to it as the video that Joanne Mettler, a pediatric nurse, identified as a minor. (*Id.*). Ms. Mettler, in her testimony, identified the subject of the video admitted as Exhibit 105/105-A, (ER 78; 9/26/12 RT 20), the video Logan purportedly downloaded through RoundUp. (ER 137; 9/24/12 RT 199).

peer-to-peer programs, which download from multiple sources. (ER 281; Government Hearing Exhibit 2); *See Chiaradio*, 684 F.3d at 271 (noting that "when a user of the commercially available version of LimeWire tries to download a file, the program seeks out all the users who are sharing the same file and downloads different pieces of that file from multiple locations in order to optimize download speed."). Logan even confirmed that he was identifying two different computers at the time he downloaded the files. (ER 121; 9/24/12 RT 183).

Despite this and without any basis, Logan testified that RoundUp could download from a single source. (ER 150--; 9/24/12 RT 212). Logan was, however, utterly unqualified to render this opinion. He testified that he did not know how RoundUp was written, its specifications, or whether the program had been tested by any independent third parties. (ER 146; 9/24/12 RT 208). Nor did he know RoundUp's error rates or whether his agency had ever produced a test or validation report. (ER 147; 9/24/12 RT 209). RoundUp is not commercially available. (ER 145-6; 9/24/12 RT 207-8).

Logan was clearly incapable of vouching for RoundUp's reliability. As a result, this Court in confronted with a very different trial record than was the First Circiut in *United States v. Chiaradio*, 684 F.3d 265. In *Chiaradio*, the First Circuit found sufficient the case agent's testimony at the *Daubert* hearing concerning the reliability of EP2P, the FBI's file sharing investigative software, because

> he had significant specialized experience with both EP2P and the manual re-creation of EP2P sessions. He testified that the program, with respect to identifying the source of particular files, had no error rate. He also demonstrated how the results of an EP2P investigation could be independently verified and made it clear that EP2P had never yielded a false positive.

684 F.3d at 278.

Despite a lack of evidence from which to conclude that RoundUp was reliable, the government argued, in summation, that it was reliable: "the hash values, that mathematical algorithm, that digital fingerprint for data that tells you that the files Special Agent Logan got from the defendant's computer, was an exact copy of the file that was on the defendant's computer" (ER 77; 9/27/12 RT 32).

Instead of taking any steps to require the government to demonstrate that RoundUp was reliable, the district court relied on a one-page announcement posted by the software developer. (ER 172; CR 69). The district court utterly abdicated its responsibility as a gatekeeper and simply took "the expert's word for it" something this Court has found to be "not enough." *Daubert*, 43 F.3d at 1319. From this source single-page source, the district court concluded that the reliability of the software was beyond cavil: "And so this is a tool that was developed by law enforcement. It was developed in an academic setting. It was funded by the National Science Foundation. It has been used extensively not only by various

police agencies but also has been the basis for courts issuing search warrants[.]" (ER 66; 9/17/12 RT 31).

Conclusion

For the reasons set forth above, the Court should find that the district court erred when it denied Mr. Dreyer's motion to suppress the fruits of the NCIS investigation, the state search warrant, and the onsite search of the desktop computer and that it erred in admitting evidence obtained and authenticated throght RoundUp, vacate Mr. Dreyer's convictions, and remand for further proceedings.

DATED: September 20, 2013.

Respectfully submitted,

s/Erik B. Levin
Erik B. Levin
Attorney for Michael Allan Dreyer

Certificate of Compliance

Pursuant to Ninth Circuit Rule 32(e)(3), I certify that this brief is proportionately spaced using 14 point Times New Roman and consists of 10,280 words.

DATED: September 20, 2013.

s/Erik B. Levin
Erik B. Levin

Certificate of Related Cases

Counsel is not aware of any related cases now pending before this Court.

DATED: September 20, 2013.

s/Erik B. Levin
Erik B. Levin

Certificate of Service

I hereby certify that on September 20, 2013, I filed the foregoing **Defendant-Appellant's Opening Brief** with the Clerk of the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system.

I certify that all non-sealed Excerpts of Record were electronically filed on this date.

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: September 20, 2013.

s/Erik B. Levin
Erik B. Levin