FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, *Plaintiff-Appellant*, v. JOSEPH T. SCHESSO, *Defendant-Appellee*.	No. 11-30311 D.C. No. 3:11-cr-05285-RJB-1 OPINION

Appeal from the United States District Court
for the Western District of Washington
Robert J. Bryan, Senior District Judge, Presiding

Argued and Submitted
June 6, 2013—Seattle, Washington

Filed September 18, 2013

Before: Ronald Lee Gilman,[*] M. Margaret McKeown,
and Sandra S. Ikuta, Circuit Judges.

Opinion by Judge McKeown

---

[*] The Honorable Ronald Lee Gilman, Senior Circuit Judge for the U.S. Court of Appeals for the Sixth Circuit, sitting by designation.

SUMMARY[**]

Criminal Law

The panel reversed the district court's grant of a suppression motion in a case in which officers found 3,400 electronic images and 632 electronic videos of commercial child pornography pursuant to a warrant authorizing an electronic search of all of the defendant's computer equipment and digital storage devices.

The panel held that because there was a fair probability that evidence of child pornography would be found on the defendant's computer system, the underlying facts supported a finding of probable cause; that the warrant was not overbroad and did not raise the risks inherent in over-seizing that this court considered in *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162 (9th Cir. 2010) (en banc) (per curiam); and that the absence of precautionary search protocols was not fatal here.

COUNSEL

Helen J. Brunner (argued), Assistant United States Attorney, Jenny A. Durkan, United States Attorney, Office of the United States Attorney, Seattle, Washington, for Plaintiff-Appellant.

[**] This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

Colin A. Feiman (argued), Assistant Federal Public Defender, Alan Zarky, Research & Writing Attorney, Federal Public Defender, Tacoma, Washington, for Defendant-Appellee.

OPINION

McKEOWN, Circuit Judge:

Searches of electronic records pose unique challenges for "striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures." *United States v. Comprehensive Drug Testing, Inc.* ("*CDT III*"), 621 F.3d 1162, 1177 (9th Cir. 2010) (en banc) (per curiam). This is a recurring theme in our decisions. *See, e.g.*, *United States v. Cotterman*, 709 F.3d 952, 957 (9th Cir. 2013) (en banc) (highlighting "individual privacy interests in data on portable digital devices" as one basis for requiring the government to have reasonable suspicion for the forensic examination of a laptop). Because electronic devices could contain vast quantities of intermingled information, raising the risks inherent in over-seizing data, *CDT III*, 621 F.3d at 1177, law enforcement and judicial officers must be especially cognizant of privacy risks when drafting and executing search warrants for electronic evidence. We addressed this issue in *CDT III*, where we considered "the reality that over-seizing is an inherent part of the electronic search process," and held that this "reality" called for judicial officers to exercise "greater vigilance" in protecting against the danger that the process of identifying seizable electronic evidence could become a vehicle for the government to gain access to a larger pool of data that it has no probable cause to collect. *Id.* *CDT III* amended an earlier pending en banc decision that

was issued a year before in 2009. *United States v. Comprehensive Drug Testing, Inc*. ("*CDT II*"), 579 F.3d 989 (9th Cir. 2009) (en banc) (revised and superseded by *CDT III*). Our case, involving a search conducted in June 2010, falls in the twilight zone between those two decisions.

We now consider the implications of *CDT III* for Joseph Schesso, at whose residence law enforcement officers found 3,400 electronic images and 632 electronic videos of commercial child pornography pursuant to a warrant authorizing an electronic search of all of Schesso's computer equipment and digital storage devices. Because there was a fair probability that evidence of child pornography would be found on Schesso's computer system, the underlying facts supported a finding of probable cause. The warrant was not overbroad and did not raise the risks inherent in over-seizing that we considered in *CDT III*. The absence of precautionary search protocols, suggested as guidance in the plurality's concurring opinion in *CDT III*, was not fatal here. We therefore reverse the district court's grant of the motion to suppress.

BACKGROUND

In the fall of 2008, German authorities conducted an investigation into the online distribution of child pornography over a decentralized peer-to-peer file-sharing network known as "eDonkey." The network allows users to share files over the Internet by connecting directly to each other's computers. The investigation revealed, and later examination confirmed, that during a four-hour period in October 2008, an 18-minute child pornography video was made available for download over eDonkey by someone using an Internet Protocol ("IP") address—a unique, electronic numeric label linked to a

specific device—located in the United States. German authorities advised Immigration and Customs Enforcement ("ICE") of this evidence and ICE Special Agent Julie Peay determined that the IP address was assigned to Schesso at his Vancouver, Washington, residence.

Detective Patrick Kennedy and Senior Digital Forensics Investigator Maggi Holbrook of the Vancouver Police Department assumed leadership of the investigation because the state had an independent interest in the crimes under investigation. Detective Kennedy, the case agent, prepared an affidavit supporting a warrant application to search Schesso's residence and seize evidence of violations of Washington statutes prohibiting possession of and dealing in child pornography. The application described the storage capacity of computers, the use of the Internet to distribute child pornography, the operation of peer-to-peer networks, and the known characteristics of child pornography collectors, such as their tendency to conceal sexually explicit images of children from discovery and to retain them indefinitely. The application further explained that due to the volume of evidence, the vulnerability of digital data, and the technical equipment and expertise needed to search digital devices, it would be necessary to remove the devices from the residence and conduct analysis and recovery of data off-site in a controlled laboratory environment.

A Washington state court judge approved the warrant in June 2010. The warrant noted that there was probable cause to search for evidence of dealing in and possession of child pornography, and authorized a search of Schesso's residence for "[a]ny computer or electronic equipment or digital data storage devices that are capable of being used" for those violations. The warrant permitted seized items to be

transferred to the Vancouver Police Department Digital Evidence Cybercrime Unit or to any qualified law enforcement digital evidence processing lab for examination, analysis, and recovery of data. The warrant did not contain any protocols for sifting through the data or any provision for the return of non-evidentiary property.

Officers from the Vancouver Police Department and ICE Agent Peay executed the warrant on the same day. The officers entered the residence when no one was home. Schesso and his wife arrived within an hour. Though not under arrest, Schesso consented to an interview after waiving his rights under *Miranda v. Arizona*, 384 U.S. 486 (1966), and admitted to viewing child pornography on and off for several years as well as to using eDonkey and other peer-to-peer software to download child pornography. Schesso estimated he had between 100 and 500 videos and between 500 and 1,000 images of child pornography, an estimate that he raised to 10,000 images at a follow-up interview the next day. Schesso's wife also called Detective Kennedy on the evening of the search to inform him that she had learned that her niece had been touched sexually by Schesso about five years earlier.

The first search of Schesso's home resulted in the seizure of multiple pieces of electronic media and data storage devices pursuant to the terms of the warrant, including a custom-built computer tower and external storage devices such as camera memory cards. The forensic examination of these devices, conducted by Investigator Holbrook, revealed 3,400 images and 632 videos of commercial child pornography, including the video that German authorities determined had been shared over eDonkey. Analysis of a camera memory card also uncovered six deleted sexually

explicit images of a young girl, later identified as Schesso's niece. Schesso's wife identified the couch and blanket depicted in those images as items in her home, and a second state search warrant was obtained to seize the blanket and a fabric sample from the couch. Investigator Holbrook halted her computer examination before completion because sufficient evidence had been found for prosecution and other cases required her attention.

The case was accepted for federal prosecution and Schesso was charged with production, distribution, receipt, and possession of child pornography in violation of 18 U.S.C. §§ 2251 and 2252A.[1] Schesso moved to suppress all evidence seized from his residence, as well as his inculpatory statements and the items seized during the execution of the second warrant, as fruits of the allegedly illegal first search. Schesso's motion focused on the procedural safeguards under *CDT III* and the staleness of the warrant. Except as to the camera memory cards, he did not challenge probable cause. His motion acknowledged that "[t]he information in the application, if it had been timely, would have provided a basis for seizing Mr. Schesso's personal computers and related storage devices."

The district court initially granted the suppression motion as to all evidence seized pursuant to the two searches, but not as to Schesso's inculpatory statements. Schesso was unsuccessful in his arguments that the warrant was invalid due to staleness and that the government had acted in bad faith by seeking the warrant from a state judge rather than a federal judge. Nevertheless, the district court concluded that

[1] Later, Schesso was also charged with child molestation in violation of Revised Code of Washington § 9A.33.083.

the affidavit failed to connect generalized statements about child pornography collectors to Schesso, thus rendering the warrant facially deficient and the good faith exception inapplicable.

The district court later issued a supplemental memorandum opinion that granted the suppression motion as to all evidence seized during both searches and as to Schesso's inculpatory statements. Although the oral ruling and earlier order expressed that the government did not engage in the type of "deliberate overreaching" that *United States v. Tamura*, 694 F.2d 591 (9th Cir. 1982), and *CDT III* intended to prevent, the opinion emphasized that the warrant application failed to include any of the protocols for searching electronic records suggested by the concurring opinion in *CDT III*. The court rejected the good faith exception to the exclusionary rule on the ground that "the overturned warrant is so facially deficient that reliance on it is not reasonable."

The government now appeals the district court's suppression ruling. Schesso's trial is stayed pending this interlocutory appeal. We review de novo the district court's grant of a motion to suppress and its application of the good faith exception to the exclusionary rule. *United States v. Maddox*, 614 F.3d 1046, 1048 (9th Cir. 2010); *United States v. Crews*, 502 F.3d 1130, 1135 (9th Cir. 2007). We review for clear error whether the state court judge issuing the warrant had a substantial basis for concluding that probable cause existed and give "great deference" to such a finding. *United States v. Hay*, 231 F.3d 630, 634 n.4 (9th Cir. 2000) (citation omitted).

ANALYSIS

I. VALIDITY OF THE SEARCH WARRANT

A. PROBABLE CAUSE

We disagree with the district court's conclusion that the warrant was facially overbroad and thus not supported by probable cause. In a somewhat unusual posture, the defense essentially conceded probable cause for the seizure, arguing that "the overriding problem was not the initial seizure of Mr. Schesso's devices, but the lack of any guidance or limits in the warrant for subsequently searching the intermingled data that was on them." Our review of the record reveals that the facts cited in the affidavit, combined with reasonable inferences drawn from those facts, provided probable cause to search Schesso's entire computer system and his digital storage devices for any evidence of possession of or dealing in child pornography.

There is no question that there was probable cause to believe that Schesso possessed the particular child pornography video uploaded to eDonkey in October 2008. Given the circumstances of that upload and the information supplied in the warrant application, the state court judge permissibly drew the "reasonable inference" that there was probable cause to believe Schesso had other child pornography materials as well. *Illinois v. Gates*, 462 U.S. 213, 240 (1983).

Schesso did not merely possess a commercial child pornography video, which might have resulted from a one-time accidental download or inadvertent receipt. Key to the probable cause analysis is the evidence that Schesso took the

affirmative step of uploading and distributing the video on a network designed for sharing and trading.[2] As the affidavit explained, peer-to-peer file sharing networks are "frequently used to trade digital files of child pornography," "often provide enhanced capabilities to reward those who share files by providing reduced wait periods, higher user ratings, or other benefits," and sometimes do not allow users to download files at all unless they also share files. It is hardly a leap to infer that Schesso either had other files to share or that he used the network to download files.

The judge issuing the warrant thus made the "practical, common-sense decision" that "given all the circumstances set forth in the affidavit before him . . . there [was] a fair probability that contraband or evidence" of child pornography would be found on Schesso's computer and other digital storage equipment. *Id.* at 238. This determination is in line with our precedent. *See, e.g.*, *United States v. Gourde*, 440 F.3d 1065, 1069–71 (9th Cir. 2006) (en banc) (emphasizing that probable cause means "fair probability," not certainty or even a preponderance of the evidence, and concluding that it was reasonable to infer that there was a fair probability that defendant "received or downloaded" child pornography images based on defendant's paid subscription to a child pornography website); *United States v. Kelley*, 482 F.3d 1047, 1053 (9th Cir. 2007) (concluding that it was reasonable to infer that defendant "was part of a network of

[2] The district court confused the act of downloading a file with the act of uploading a file. In his oral ruling, he inaccurately stated that "[t]he only crimes described . . . in the affidavit are the possession and downloading of [one] particular file." Not so. In fact, the scope of the warrant is specifically premised on Schesso's *uploading* of the file, an act that connects him to the profile of a child pornography collector.

persons interested in child pornography" and permissible to search defendant's computer based on evidence that defendant had received nine emails with attachments "containing the same type of illicit child pornography" that was found on the computers of two individuals who collected or distributed child pornography); *United States v. Lacy*, 119 F.3d 742, 745 (9th Cir. 1997) (implying that it was reasonable to infer that defendant had the characteristics of a "collector[] of child pornography" based on evidence in the affidavit that defendant had downloaded at least two computerized visual depictions of child pornography).

Because there was a fair probability that the eDonkey video as well as other evidence of possession of and dealing in child pornography would be found on Schesso's digital equipment, the warrant was not overbroad. The government was faced with the challenge of searching for digital data that was not limited to a specific, known file or set of files. The government had no way of knowing which or how many illicit files there might be or where they might be stored, or of describing the items to be seized in a more precise manner. *United States v. Adjani*, 452 F.3d 1140, 1447–48 (9th Cir. 2006) ("Warrants which describe generic categories of items are not necessarily invalid if a more precise description of the items subject to seizure is not possible.") (citation omitted). These factors, along with the detailed explanation of the need for off-site analysis and recovery, justify the seizure and subsequent off-premises search of Schesso's entire computer system and associated digital storage devices.[3]

[3] This process is not out of the ordinary. Federal Rule of Criminal Procedure 41(e)(2)(B) explicitly permits the seizure or copying of electronically stored information for later off-site review.

We have repeatedly found equally broad searches constitutional on similar or less evidence. *See, e.g.*, *United States v. Krupa*, 658 F.3d 1174, 1178 (9th Cir. 2011) (holding valid a search of fifteen computers at a residence based on evidence of one contraband image and a report of child neglect); *United States v. Brobst*, 558 F.3d 982, 993–94 (9th Cir. 2009) (holding valid a warrant authorizing the search and seizure of photographs, computers, compact disks, floppy disks, hard drives, memory cards, printers, other portable digital devices, DVDs, and video tapes based on a witness's observation of one illicit photograph in defendant's home); *Lacy*, 119 F.3d at 746 (9th Cir. 1997) (holding valid a warrant authorizing the "blanket seizure" of Lacy's "entire computer system" because the government did not know where at least two illicit child pornography images were stored and "no more specific description of the computer equipment sought was possible").

We are not convinced by Schesso's additional argument that there was no probable cause to seize the camera memory cards simply because Schesso was not suspected of producing child pornography. Camera memory cards have data storage functionality like any external digital storage device, and Schesso's custom-built computer tower had a port connecting directly to camera memory cards, allowing him to read, write, or import data between devices. At the time of the search, a camera was connected to one of the computers. The officers reasonably concluded that the camera memory cards were covered by the warrant as "digital data storage devices . . . capable of being used to commit or further" the crimes of possession of and dealing in child pornography.

Nor are we persuaded that the information supporting the warrant application was stale. Information underlying a

warrant is not stale "if there is sufficient basis to believe, based on a continuing pattern or other good reasons, that the items to be seized are still on the premises." *Lacy*, 119 F.3d at 745–46 (internal quotation marks and citation omitted). Such good reasons existed here: Detective Kennedy's affidavit explained that individuals who possess, distribute, or trade in child pornography "rarely, if ever, dispose of sexually explicit images of children" because these images are treated as "prized possessions." In light of the "nature of the criminal activity and property sought" and the reasonable inference that Schesso fit the profile of a collector, the state court judge had ample reason to believe that the eDonkey video or other digital child pornography files would be present at Schesso's residence a mere 20 months after the eDonkey incident. *Id.* at 745 (citation omitted); *see also United States v. Allen*, 625 F.3d 830, 842–43 (5th Cir. 2010) (holding that an 18-month delay between when defendant sent child pornography images through a peer-to-peer networking site and issuance of a search warrant did not render the information stale); *United States v. Morales-Aldahondo*, 524 F.3d 115, 117–19 (1st Cir. 2008) (concluding that the passage of over three years since the acquisition of information that defendant's brother, who shared defendant's residence, had purchased access to various child pornography websites, did not render that information stale).

Given these circumstances and the details contained in the affidavit, the state court judge had a substantial basis for and did not commit clear error in determining that there was probable cause for the warrant. We defer to that judgment.

B. ABSENCE OF SEARCH PROTOCOL

The question we consider next is whether the electronic data search guidelines laid out in the *CDT* cases affect the outcome here. After considering constitutional requirements, the temporal sequence of the cases, and the advisory nature of the guidelines, we conclude that the absence of these protocols in Schesso's warrant neither violates the Fourth Amendment nor is inconsistent with *CDT III* or its predecessor case, *Tamura*. Schesso's scenario did not implicate the real concern animating the court in *CDT III* and *Tamura*: preventing the government from overseizing data and then using the process of identifying and segregating seizable electronic data "to bring constitutionally protected data into . . . plain view." *CDT III*, 621 F.3d at 1171 (per curiam opinion).

In *Tamura*, the government had probable cause to seize three categories of paper records. To avoid the time-consuming task of identifying those specific records on site, the government seized substantially more records for off-site examination, thus gaining access to materials it had no probable cause to collect. *Tamura*, 694 F.2d at 594–95. Significantly, the seizure far exceeded the documents detailed in the warrant. Our analysis was blunt: "It is highly doubtful whether the wholesale seizure by the Government of documents *not mentioned in the warrant* comported with the requirements of the fourth amendment." *Id.* at 595 (emphasis added). Although we declined to suppress the evidence at trial, we suggested procedural safeguards and monitoring by a magistrate when over-seizure is justified because documents subject to seizure "are so intermingled" that they cannot feasibly be identified and segregated on-site. *Id.* at 595–96.

In *CDT III*, we reiterated the concerns expressed in *Tamura* in the context of electronic data. A short procedural history of *CDT III* is in order. During the time government agents were investigating Schesso, our court issued its original en banc decision, now known as *CDT II*, in a case involving steroid use by professional baseball players. The government had probable cause to seize the electronic drug testing records of ten baseball players from an independent company administering the drug testing program. *CDT III*, 621 F.3d at 1166. But the government requested authorization to seize considerably more data beyond that of the ten players for off-site segregation and examination. *Id.* at 1168. The magistrate judge granted the request subject to the government's following certain procedural safeguards "designed to ensure that data beyond the scope of the warrant would not fall into the hands of the investigating agents"—including that "law enforcement personnel trained in searching and seizing computer data," rather than investigating case agents, conduct the initial review and segregation of data. *Id.* at 1168–69.

Once the electronic data was seized, however, the government ignored the required protocols. Alongside the computer specialist, the investigating case agent reviewed the drug testing results of hundreds of professional athletes for whom probable cause had not been shown, and used what he learned to obtain subsequent search warrants based on the government's contention that the evidence was in "plain view." *Id.* at 1170–72. Referencing the district court's binding order that the government intentionally disregarded the warrant's procedural safeguards, we affirmed the district court's grant of the motion to return the records of all but the ten identified baseball players who had been suspected of

criminal activity.[4] *Id.* at 1174. To avoid a reprise, *CDT II* laid out a number of procedural safeguards for future warrants as part of the majority opinion.[5]

After *CDT II*, magistrate judges in the Western District of Washington took steps to implement the protocol, requiring the protocol for all warrants authorizing searches of electronically stored information. Because the government disagreed with this approach, ICE directed its agents not to agree to a waiver of plain view, for example, and adopted a practice of submitting its warrant applications to state judges rather than through the federal system.

Approximately a year later, the en banc court issued a new, amended opinion. The search protocol was no longer part of the majority opinion, but instead was moved to a concurring opinion and thus was no longer binding circuit precedent. By its own terms, the concurring opinion proposes the protocols not as constitutional requirements but as "guidance," which, when followed, "offers the government a safe harbor." *CDT III*, 621 F.3d at 1178 (Kozinski, C.J., concurring). Notably, there is no clear-cut rule: "District and magistrate judges must exercise their independent judgment in every case, but heeding this guidance will significantly increase the likelihood that the searches and seizures of

[4] We laid out three alternative reasons for affirming the district court's grant of the motion to return. The other two reasons were preclusive effect and equitable considerations.

[5] These prophylactic guidelines include waiver of reliance on the plain view doctrine, segregation and redaction of electronic data by specialized personnel or an independent third party, and disclosure of the actual risks of destruction of information. *CDT II*, 579 F.3d at 1006.

electronic storage that they authorize will be deemed reasonable and lawful." *Id.*

Schesso's situation is unlike *CDT III* and *Tamura* in that the government properly executed the warrant, seizing only the devices covered by the warrant and for which it had shown probable cause. Based on the evidence that Schesso possessed and distributed a child pornography video on a peer-to-peer file-sharing network, law enforcement agents had probable cause to believe that Schesso was a child pornography collector and thus to search Schesso's computer system for any evidence of possession of or dealing in child pornography. In other words, Schesso's entire computer system and all his digital storage devices were suspect.

Tellingly, the search did not involve an over-seizure of data that could expose sensitive information about other individuals not implicated in any criminal activity—a key concern in both the per curiam and concurring opinions of *CDT III*[6]—nor did it expose sensitive information about

[6] "Electronic storage and transmission of data is no longer a peculiarity or a luxury of the very rich; it's a way of life. Government intrusions into large private databases thus have the potential to expose exceedingly sensitive information about countless individuals not implicated in any criminal activity, who might not even know that the information about them has been seized and thus can do nothing to protect their privacy." *CDT* III, 621 F.3d at 1177 (per curiam opinion) (rejecting the argument that people can avoid the potential that government over-seizure of electronic data could expose their private information simply by not storing their data electronically). The *CDT III* concurrence recommended that "where the party subject to the warrant is not suspected of any crime, and where the privacy interests of numerous other parties who are not

Schesso other than his possession of and dealing in child pornography. Indeed, inclusion of the search protocols recommended in the *CDT III* concurrence would have made little difference for Schesso. For example, the concurrence recommends that the government forswear reliance on the plain view doctrine, or have an independent third party segregate seizable from non-seizable data. *Id.* at 1178. Here, officers never relied on the plain view doctrine; they had probable cause to search for child pornography, and that is precisely what they found. The seized electronic data was reviewed by Investigator Holbrook, a specialized computer expert, rather than Detective Kennedy, the case agent, and Schesso does not assert that Holbrook disclosed to Kennedy "any information other than that which [was] the target of the warrant." *Id.* at 1180. Additionally, unlike the concern articulated in the concurrence in *CDT III*, which stated that the affidavit created the false impression that the data would be lost if not seized at once,[7] here the affidavit explained that individuals who possess, distribute, or trade in child pornography "go to great lengths to conceal and protect from discovery their collection of sexually explicit images of minors."

---

under suspicion of criminal wrongdoing are implicated by the search, the presumption should be that the segregation of the data will be conducted by an independent third party selected by the court." *Id.* at 1179 (Kozinski, C.J., concurring).

[7] According to the concurrence, the independent business that owned the data was not a criminal suspect and had agreed to keep the data intact, a representation the United States Attorney's Office had accepted. *Id.* at 1178 (quoting the dissent in *United States v. Comprehensive Drug Testing*, 513 F.3d 1085, 1132 (9th Cir. 2008) (Thomas, J., dissenting), opinion revised and superseded by *CDT III*).

Although we conclude that the exercise of "greater vigilance" did not require invoking the *CDT III* search protocols in Schesso's case, judges may consider such protocols or a variation on those protocols as appropriate in electronic searches. We also note that Rule 41 of the Federal Rules of Criminal Procedure sets forth guidance for officers seeking electronically stored information.[8] Ultimately, the proper balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures of electronic data must be determined on a case-by-case basis. The more scrupulous law enforcement agents and judicial officers are in applying for and issuing warrants, the less likely it is that those warrants will end up being scrutinized by the court of appeals.

II. SUPPRESSION OF EVIDENCE

Even if the warrant were deficient, the officers' reliance on it was objectively reasonable and the "good faith" exception to the exclusionary rule applies. *United States v. Leon*, 468 U.S. 897, 922 (1984) ("[T]he marginal or nonexistent benefits produced by suppressing evidence

[8] As amended, Rule 41 provides, among other procedures, that a warrant seeking electronically stored information "may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant." Fed. R. Crim. P. 41(e)(2)(B). Upon executing the warrant, "[i]n a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied." Fed. R. Crim. P. 41(f)(1)(B).

obtained in objectively reasonable reliance on a subsequently invalidated search warrant cannot justify the substantial costs of exclusion."). The state court judge was not misled by information in the affidavit, he did not wholly abandon his judicial role, and the affidavit certainly was not "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." *Id.* at 923 (quoting *Brown v. Illinois*, 422 U.S. 590, 611 (1975) (Powell, J., concurring in part)).

The rationale leading us to defer to the state court judge's determination of probable cause applies with even greater force to the question whether the officers' reliance on the warrant was objectively reasonable. The affidavit included sufficient evidence connecting Schesso to the profile of a child pornography collector to justify the officers' reliance on the warrant. We have previously upheld comparably broad warrants based on similar evidence. *See, e.g.*, *Krupa*, 658 F.3d at 1178; *Brobst*, 558 F.3d at 993–94.

Our analysis is not affected by the officers' decision to seek a warrant from a Washington state court rather than the Western District of Washington. We recognize that the choice of forum was influenced by the Western District of Washington's policy at the time of requiring the search protocols outlined in *CDT II*. But evidence should be suppressed "only if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment." *Herring v. United States*, 555 U.S. 135, 143 (2009) (quoting *Illinois v. Krull*, 480 U.S. 340, 348–49 (1987)). Because neither *CDT II* nor *CDT III* cast the search protocols in constitutional terms, state judicial officers cannot be faulted for not following protocols that were not binding

on them, and law enforcement officers cannot be faulted for relying on a warrant that did not contain the non-binding protocols.[9] Nothing prohibits the government from seeking a warrant from one forum over another where the government has the option to prosecute the case in state or federal court. The Fourth Amendment applies equally to state courts as to federal courts. The constitutionality of a warrant is not forum dependent.

REVERSED.

[9] It bears noting that neither *Tamura* nor *CDT III* resulted in the suppression of evidence despite the absence of precautionary procedures. We declined to suppress evidence in *Tamura* because although the search exceeded the scope of the warrant, the specific documents introduced at trial were within its scope. *Tamura*, 694 F.2d at 597 ("Generally, the exclusionary rule does not require the suppression of evidence within the scope of a warrant simply because other items outside the scope of the warrant were unlawfully taken as well."). *CDT III* did not concern a motion to suppress at all. Rather, compliance with *Tamura* was discussed in the context of a motion to return property under Federal Rule of Criminal Procedure 41(g), which is "broader than the exclusionary rule." *CDT III*, 621 F.3d at 1173 (per curiam opinion).