UNIVERSAL CASE OPINION COVER SHEET

U.S. District Court for the Central District of Illinois

Complete TITLE of Case	**UNITED STATES OF AMERICA,** **Plaintiff,** **v.** **CHRISTOPHER OWEN SCHLINGLOFF,** **Defendant.**	
Type of Document	**ORDER**	
Docket Number	Case No. 11-40073	
COURT	UNITED STATES DISTRICT COURT FOR THE CENTRAL DISTRICT OF ILLINOIS - ROCK ISLAND DIVISION	
Opinion Filed	Date: October 23, 2012	
JUDGE	Honorable James E. Shadid 204 U.S. Courthouse 100 N.E. Monroe Peoria, IL 61602 (309) 671-4227	
ATTORNEYS For Plaintiff	John K. Mehochko	**Assistant United States Attorney** 1830 2nd Avenue Rock Island, IL 61201-8003
ATTORNEYS For Defendant	George F. Taseff	**Federal Public Defender** Suite 1500 401 Main St. Peoria, IL 61602

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF ILLINOIS

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Case No. 11-40073
	)	
CHRISTOPHER OWEN SCHLINGLOFF,	)	
	)	
Defendant.	)	

O R D E R

This matter was before the Court on May 16, 2012, for a hearing on Defendant, Christopher Schlingloff's ("Schlingloff"), Motion to Suppress Evidence. After hearing evidence and considering the arguments presented, the Court denied the Motion to Suppress Evidence. Defendant filed a Motion to Reconsider. After hearing oral argument on the Motion to Reconsider, the Court finds that the Motion to Reconsider [22] is GRANTED. The May 23, 2012 Order [19] is VACATED and superceded by this Order.

BACKGROUND

On November 3, 2010, agents obtained a warrant to search the residence located at 1816 2nd Avenue, Rock Island, Illinois, for evidence of passport fraud and harboring an alien. The affidavit indicated that there was reason to believe that computer devices found in the residence would contain records related to these crimes due to the fact that one target of the investigation had used computer devices in the past to generate, store, and print documents used in the passport scheme. Schlingloff was not the target of the

investigation but was present in the residence at the time the warrant was executed and informed agents that he was living there with the targets. Approximately 130 media devices were seized during the search, including a laptop and external storage device belonging to Schlingloff; these items were sent to the DSS Computer Investigations and Forensics Division office in Arlington, Virginia, for analysis.

In December 2010, Agent Scott McNamee, a computer forensic analyst, began to examine the seized devices. In doing so, McNamee used a computer software program known as Forensic Tool Kit or FTK to index/catalog all of the files on the devices into viewable formats. The Known File Filter or KFF in the software was enabled to flag and alert during processing to certain files that are identifiable from a library of known files previously submitted by law enforcement, such as contraband or child pornography. McNamee described enabling the KFF alert as his standard operating procedure. The KFF alert in this case identified to two video files entitled "Vicky" as child pornography. Based on his investigation of one to two dozen child pornography cases in the past, McNamee suspected that the file scontained child pornography and briefly opened the files to confirm his belief. McNamee observed the image of a naked prepubescent girl and an adult male, closed the file, and stopped any further processing of both the laptop and the external storage device. He then notified Agent Michael Juni about his discovery.

Based on this information, Juni prepared an application for search warrant to search the laptop and external storage device for evidence of receipt and possession of child pornography. A search warrant issued on February 4, 2011, and a total of 33 video

files containing known child pornography were found on these two devices. Files were also found indicating that Schlingloff was the owner and operator of the two devices.[1]

On July 21, 2011, Schlingloff was interviewed by the police and admitted to downloading and viewing child pornography on the laptop in question. On August 17, 2011, Schlingloff was indicted on one count of possession of child pornography in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2). Schlingloff moved to suppress the evidence found during the forensic examination of his laptop and external storage device. The Court initially denied the Motion to Suppress based in part on the mistaken belief that the filters in the FTK system had to be applied on an all or nothing basis and that the agent lacked the ability to disable the portion of the KFF specifically alerting to known child pornography or other contraband and in part on a distinction from the facts in *Mann* that the Court no longer finds persuasive in the totality of the circumstances. Schlingloff then filed a Motion to Reconsider, bringing the factual error to the Court's attention and making it clear that the KFF alerts can be disabled or not affirmatively enabled as part of the processing with very little effort. Oral argument was held, and this Order follows.

DISCUSSION

Under the Fourth Amendment, search warrants must describe the things to be seized "with sufficient particularity to prevent a general exploratory rummaging through one's belongings." *United States v. Mann*, 592 F.3d 779, 782 (7th Cir. 2010), *citing Marron v. United States*, 275 U.S. 192, 196 (1927). Schlingloff's argument is essentially

[1] A third search warrant was subsequently obtained to search the remaining devices from the initial seizure for evidence of child pornography, but that warrant is not at issue in the current case.

that the use of the KFF filter in the FTK program to flag known files containing child pornography enabled the agents to unreasonably broaden a limited search for evidence of passport fraud into a general search for evidence of any illegal activity.

Both the Government and Schlingloff rely on *Mann* in support of their arguments despite the fact that they reach opposite conclusions. Perhaps this is because *Mann* is a very fact-driven opinion that also expressly acknowledges that inquiries of this nature are inherently fact intensive. It is these factual distinctions that compel the result in this case.

To the extent that Schlingloff suggests that the use of the FTK software in and of itself exceeded the scope of the warrant per se, his argument is unpersuasive. The Seventh Circuit has held that the use of the FTK filtering software to index and catalogue files into a viewable format does not, in and of itself, exceed the scope of a warrant based on the fact that digital evidence could be found virtually anywhere on a computer. *Mann*, 592 F.3d at 784.

Schlingloff further argues that : (1) even if the use of the FTK software in and of itself is not problematic, enabling the KFF alerts in cases that do not involve suspected child pornography or some closely related cause of action necessarily broadens the scope of the search in an unconstitutional manner, and/or (2) the opening of the child pornography files by Agent McNamee takes the search beyond the scope of the warrant. These are the main issues addressed here.

McNamee concedes that despite his understanding that he was searching for evidence of passport fraud or identity theft, he consciously and affirmatively checked the box to include the KFF alerts for child pornography because that is his standard operating procedure.

Q. (By Mr. Tasseff) [Y]ou wouldn't have received those alerts had you restricted your search for the objects of the warrant and clicked the hide button for KFF Alert, correct?

A. (By Agent McNamee) I would not have clicked on the KFF.

Q. You didn't in this instance, correct?

A. No, I clicked to include the KFFs. . . .

Q. You went ahead and did that because that's your standard operating procedure, isn't it?

A. Yes.

Q. The 30 some cases that you have done, you have done it every time, correct?

A. Correct.

Q. Does your agency investigate strictly child porn cases?

A. No, it does not.

Q. In fact, this child porn case is a rare exception to the general rule, isn't it?

A. Yes. . . .

Q. But you used the forensic tool that alerted you to the presence of child porn in a non-porn case, didn't you sir?

A. Correct.

(Transcript 71-77)

McNamee's testimony and the FTK User Guide reveal that the user can either choose to apply an existing, predefined filter or customize a filter based on the purposes of the search with relative ease by checking various boxes in the setup menu. In doing so, the Court now understands that it is simple to make selections that allow the user to take advantage of the utility of the FTK program to categorize and sort out common

known files such as program files, etc., without being required to flag the KFF alerts for child pornography files as part of the process.

The search here did not end with flagging the child pornography files during preprocessing, however. After the KFF alerted to the two files in question, McNamee believed that he recognized them to be part of the "Vicky" series of child pornography based on their hash values and his experience. Rather than stopping at this point to obtain a warrant to search for images of child pornography, McNamee briefly opened each file in order to confirm his suspicions before stopping any further processing and notifying Agent Juni. When the facts of this case are considered in their totality, the Court finds that suppression is required.

The Court of Appeals has recognized that where the KFF alert flags a file as child pornography, an agent could be acting outside the scope of the warrant if he opens the flagged files without obtaining a new warrant. *Id.*, at 784-86. In fact, the Seventh Circuit suppressed the files that had been opened in *Mann*, stating:

> Once those files had been flagged, Detective Huff knew (or should have known) that files in a database of known child pornography images would be outside the scope of the warrant to search for images of women in locker rooms – presumably images that Mann himself had captured. . . . we hold that Officer Huff exceeded the scope of the warrant by opening the four flagged "KFF Alert" files.

This language in *Mann*, in conjunction with reliance elsewhere in the opinion on the agent's testimony that he "continued to look for items with voyeurism, and as I came across the child pornography, then I would not ignore it obviously" indicates that an agent does not have to be so zealous as to abandon their initial search parameters to go in search of child pornography in order to warrant suppression.

By opening the "Vicky" files flagged by the KFF alert, McNamee knew or should have known that those files would be outside the scope of the warrant to search for evidence of passport fraud or identity theft, particularly as the warrant did not specifically refer to evidence found in video files. In this respect, the facts of this case are distinguishable from either *United States v. Burgess*, 573 F.3d 1078, 1092 (10th Cir. 2009) or *United States v. Wong*, 334 F.3d 821 (9th Cir. 2003), both of which are cited favorably in Mann, where the files were opened inadvertently in the normal course of the search.

Additionally, in light of the admitted ability to confine the FTK search by not enabling the KFF filter for child pornography alerts, the Court finds that Agent McNamee took an affirmative additional step to enable the KFF alerts that would identify known child pornography files as part of his search for evidence of passport fraud or identity theft. In a case where the professed subject matter sought in the search bore no resemblance to child pornography, it is difficult to construe this as anything other than a deliberate expansion of the scope of the warrant, or at the very least, an affirmative step that effectively did so.

Given the ever increasing state of technology and consequently, technology related crimes, the Court finds that this issue is not going to go away, and in fact, will likely become more prevalent and finely contoured. Digital images or files can be located nearly anywhere on a computer and "may be manipulated to hide their true contents." 592 F.3d at 782-83, *citing United States v. Hill*, 459 F.3d 966, 978 (9th Cir. 2006). Accordingly, more comprehensive and systematic searches have been found to be reasonable. *See United States v. Grimmett*, 439 F.3d 1263, 1270 (10th Cir. 1006)(finding that a computer search may be as extensive as reasonably required to locate the items

described in the warrant.) Nevertheless, it is also important to note that there is normally no fear of degradation or dissipation of evidence or a rapidly evolving situation requiring the need to "shoot from the hip" in examining seized computer files without a proper warrant. *United States v. Seiver*, 692 F.3d 774, 777 (7th Cir. 2012). In fact, Judge Posner recently noted that the doctrine of staleness has taken on new contours as a result of technological advancements and the importance of employing a "realistic understanding of modern computer technology" when evaluating Fourth Amendment challenges to computer searches. *Id.*, at 778.

The promise of the Fourth Amendment to be free from unreasonable searches and seizures contemplates a warrant that sets forth with specificity the area to be searched and the subject matter of the search. So if a warrant authorizes an officer to look in all files on a computer, should the courts care how it is done? This Court believes so.

This caution seems particularly appropriate when considering the Government's proffered justification that the pornography files were in plain view or that they would have inevitably been discovered in a manual search. The plain view doctrine requires the officer to be where he has a right to be when he observes the evidence in plain view; the discovery must also be inadvertent. *United States v. Cooks*, 493 F.2d 668, 671 (7th Cir. 1974). The suggestion that the agent inadvertently came across a file when that same agent specifically set up the situation to find and highlight this type of file by "clicking" to enable the KFF alert is untenable.

The same follows with the argument that the files would have inevitably been discovered. The search request in this case was not limited solely to documents, but rather sought records, photographs, and evidence "in whatever form they may be kept"

on the premises that would be relevant to the crimes of passport fraud or identity theft. Given that such evidence could have been stored electronically as document files, spreadsheets, photo files, or a variety of other file types, McNamee testified that procedure would have required him to examine every file on the laptop and external storage device either manually or with the assistance of the indexing and sorting software; it would have taken much longer and consumed more manpower resources to complete the task manually, but the file would have eventually been found, and the result would have been the same. To some degree, this argument misses the point, as the use of the filter did not require McNamee to look at all; the filter locates the files and brings them to the attention of the officer. Discovery is specifically targeted rather than the result of inadvertence.

All-encompassing manual searches may be theoretically possible, yet the availability of technology and lack of manpower resources make them impractical in the average case. This is supported by McNamee's testimony where he then qualified his response to concede that his department did not have the resources to perform full, manual searches of all seized electronic devices and that as a result, manual searches would hopelessly bog down his office to the point where the examinations could not get done within the constraints of the Speedy Trial Act.

The warrant as drafted in this case is not challenged as unconstitutional. The use of the KFF alerts alone may not move this case beyond the scope of the warrant; the alert on the Vicky files alone may not move this beyond the scope of the warrant. Under some circumstances, the act of briefly opening the files to confirm their contents may not move this beyond the scope of the warrant. But combine these with the additional facts of an

agent affirmatively enabling the KFF filter to alert for child pornography in a non-pornography case that involves a search warrant seeking evidence of passport fraud and does not specifically refer to evidence in the form of videos, in conjunction with the agent opening the files once alerted to their presence, there can be no other conclusion than that the scope of the warrant was exceeded in this case.

For all these reasons, the Court agrees with Schlingloff that the scope of the warrant in this case was exceeded, thereby requiring the suppression of the opened child pornography files.[2] Any other outcome would be contrary to the intent of the Fourth Amendment that search warrants must describe with particularity the things to be seized, so that a search for specified evidence does not devolve into a generalized search for something entirely different.

CONCLUSION

For the reasons set forth above, Schlingloff's Motion to Reconsider [22] is GRANTED. The May 23, 2012 Order [19] is VACATED and superceded by this Order. As a result, Schlingloff's Motion to Suppress Evidence [15] is GRANTED.

ENTERED this 23rd day of October, 2012.

James E. Shadid
James E. Shadid
Chief United States District Judge

2 Unlike the situation in Mann, there is no other evidence of child pornography being relied on by the Government in this case upon which to effect a severance of the suppressed files.