United States v. Perez

Decided Jun 2, 2015

CRIMINAL ACTION NO. 14-611

06-02-2015

UNITED STATES v. JAVIER PEREZ

DuBois, J.

DuBois, **J**. **MEMORANDUM**

I. INTRODUCTION

Defendant Javier Perez is charged in the Indictment with two counts of distributing child pornography, in violation of 18 U.S.C. § 2252(a)(2), and one count of possessing child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B). Perez has moved to preclude the Government from introducing at trial physical evidence obtained during a search of his computer. An evidentiary hearing and oral argument on the Motion was held on May 1, 2015. For the reasons that follow, Perez's Motion is denied.

II. FACTS [1]

[1] The factual background is taken from the motion papers and the evidence presented at the May 1, 2015 hearing.

On October 15 and October 23, 2013, an undercover Federal Bureau of Investigation ("FBI") agent downloaded two files containing visual depictions of child pornography shared by a computer signed on to the Ares network.[2] An investigation of the Internet Protocol ("IP") address which shared the downloaded files revealed that it was assigned to the home of Perez. *2

2

[2] Ares is a "peer-to-peer network," which allows users to search for files being offered for sharing by others connected to the network at that time and to download files offered for sharing by connecting directly to the sharing computers. (Gov.'t Opp. to Def.'s Mot. to Suppress 2 n.1.)

On March 19, 2014, FBI Special Agent Laura Pagel submitted an affidavit and applied for a warrant to search Perez's house for items related to the possession and distribution of child pornography. A warrant authorizing the search for and seizure of, inter alia, all "visual depictions" of child pornography "on whatever medium," and documents, emails, records, notes, and other materials related to child pornography, was subsequently issued. (Def.'s Mot. to Suppress, Ex. A, 2.) On March 21, 2014, the warrant was executed, and agents seized one desktop computer and three thumbdrives from Perez's bedroom.

The Government employed the following search methodology to examine the seized items: The computer and thumbdrives were first delivered to the FBI's Computer Forensics Laboratory in Philadelphia. The first assigned case agent, Special Agent Andrea Manning,[3] requested that the forensic examiner process the

computer and thumbdrives for various types of evidence, including: graphic and video files, files which matched known child pornography images (CVIP files), internet history, internet favorites, and mobile syncs and data. The FBI examiner, after making an exact digital copy of the seized evidence, loaded the copy of the digital evidence into Forensic Toolkit ("FTK"), a forensic analysis tool. The FTK software then catalogued and segregated the requested files into a viewable format. At the May 1, 2015 hearing, FBI examiner Donald Justin Price explained that the software "scans the entire computer system. It looks at every file and folder and it identifies it based on the file type. So it'll categorize it as a document, a video, a graphic file, so on and so forth." (Hearing Tr., May 1, 2015, 17.) The forensic software also compares the extension of each file with the source information of that file to identify if there is a mismatch. The program is thus able to identify [3] and extract graphic images and video files, even if concealed in files with extensions that are not traditionally associated with those file types.

[3] Special Agent Daron Schreier became the case agent in February 2015 because Special Agent Manning was assigned to temporary duty outside of the division. (Hearing Tr., May 1, 2015, 29-30.)

The examiner then reviewed the extracted data to filter out files that clearly fell outside the scope of the case agent's request, e.g. generic application icons. The extracted data included CVIP hits, directory file listings, email, items from the recycle bin, graphic and video files, internet artifacts, and various "favorites." A digital copy of only the extracted evidence was provided to the case agent for further review.

In February 2015, Special Agent Manning asked the FBI examiner for additional information from Perez's computer and thumbdrives with respect to the Ares peer-to-peer program. The examiner followed the same protocol as was followed in the first examination, and subsequently provided Special Agent Manning with information concerning incomplete and complete Ares downloads, search terms, shared files, and the install date. The Government contends that the extracted files provided by the FBI examiner constituted only a limited portion of all the data on Perez's computer and thumbdrives.

Special Agent Manning, and subsequently Special Agent Schreier, reviewed the extracted files to determine whether they contained evidence related to the possession and distribution of child pornography. At the May 1, 2015 hearing, Special Agent Schreier testified that their examination of the extracted files consisted of the following: they viewed graphic images, including those attached to emails, in a thumbnail version, and only opened them when it was believed that they contained evidence related to child pornography; opened and played short portions of video files; opened emails without attachments only if the subject line or sender gave them reason to believe that they contained evidence of child pornography; and opened and cursorily examined other extracted file types, e.g. internet history, to determine whether those [4] files contained evidence that fell within the scope of the warrant and to identify the internet user at particular times. The case agents determined that approximately ten files on the computer contained visual depictions of child pornography. They also found a list of search terms on the computer related to child pornography, which had been used to search the Ares network software, and determined that the computer had Ares network software. The evidence was recovered from Perez's computer hard drive.

On November 13, 2014, a Grand Jury returned an Indictment charging Perez with two counts of distributing child pornography, in violation of 18 U.S.C. § 2252(a)(2), and one count of possessing child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B).

Perez filed a Motion to Suppress the seized files on April 7, 2015. On May 1, 2015, the Court held an evidentiary hearing and oral argument on the Motion.

III. LEGAL STANDARD

"On a motion to suppress, the government bears the burden of showing that each individual act constituting a search or seizure under the Fourth Amendment was reasonable." United States v. Ritter, 416 F.3d 256, 261 (3d Cir. 2005) (citing United States v. Johnson, 63 F.3d 242, 245 (3d Cir. 1995)). The government must meet this burden by a preponderance of the evidence. United States v. Matlock, 415 U.S. 164, 177 (1974).

Under the Fourth Amendment, a search pursuant to a warrant is limited to the scope of the warrant. "As to what is to be taken, nothing is left to the discretion of the officer executing the warrant." Andresen v. Maryland, 427 U.S. 463, 480 (1976) (citations and internal quotation marks omitted). "If the scope of the search exceeds that permitted by the terms of a validly issued warrant or the character of the relevant exception from the warrant requirement, the subsequent seizure is unconstitutional without more." Horton v. California, 496 U.S. 128, 140 *5 (1990). "Whether evidence is within a search warrant's scope requires not a 'hypertechnical' analysis, but a 'common-sense, and realistic' one." United States v. Okorie, 425 F. App'x 166, 169 n.1 (3d Cir. 2011) (quoting United States v. Srivastava, 540 F.3d 277, 291 (4th Cir. 2008)).

IV. DISCUSSION

In his Motion to Suppress, Perez argues that the search of his computer and thumbdrives, which consisted, in part, of "[o]pening files in order to determine their contents,"[4] was not executed in accordance with the warrant's terms, but instead was a general rummaging in violation of the Fourth Amendment.[5] At the May 1, 2015 hearing, counsel for defendant raised an additional argument — that the use of the FTK software to conduct the initial forensic examination of Perez's computer and thumbdrives exceeded the scope of the warrant in violation of the Fourth Amendment.

[4] In his Motion, Perez relies on the Search Warrant Affidavit, which sets out what the Government's search methodology "may consist of." In its Response and at the hearing held on May 1, 2015, the Government confirmed that it employed this approach as part of its search methodology.

[5] Perez does not challenge the validity of the search warrant itself.

Perez's challenges to the Government's search methodology require the Court to reconcile two competing principles: "On one hand, it is clear that because criminals can — and often do — hide, mislabel, or manipulate files to conceal criminal activity, a broad, expansive search of the hard drive may be required . . . On the other hand . . . granting the Government a carte blanche to search every file on the hard drive impermissibly transforms a limited search into a general one." United States v. Stabile, 633 F.3d 219, 237 (3d Cir. 2011) (internal citations and quotation marks omitted). Although the U.S. Court of Appeals for the Third Circuit has not yet adopted a particular method of addressing these competing principles, or reached the precise *6 questions presented in this case, the Court is guided by the Third Circuit's decision in Stabile and the cases discussed therein, which address Fourth Amendment issues in the context of computer searches. Id. The Court addresses each of Perez's arguments in turn.

i. The Government's Use of Forensic Analysis Software

Perez first argues that the Government's use of the FTK software exceeded the scope of the warrant in violation of the Fourth Amendment. The Court rejects this argument. Given the limited nature of the forensic software's examination, which consisted of cataloging and segregating files by file type into a viewable format, and the fact that Perez could have graphic and video files containing child pornography "virtually anywhere on his computer," the Court concludes that the Government did not exceed the scope of the warrant by using the FTK

software. United States v. Mann, 592 F.3d 779, 784-85 (7th Cir. 2010) (no reason to believe that detective's use of FTK software to index and catalogue files, without more, exceeded scope of warrant where search warrant authorized search and seizure of evidence of voyeurism, and images of women in locker rooms could be "virtually anywhere on his computers"); see also United States v. Schlingloff, 901 F. Supp. 2d 1101, 1103 (C.D. Ill. 2012) (rejecting argument that FTK software exceeded scope of warrant per se); United States v. Giberson, 527 F.3d 882, 889-90 (9th Cir. 2008) (upholding as reasonable a search in which Government used "ILOOK" forensic software, which, like FTK, catalogs and segregates files based on file type into viewable format, where warrant authorized search for images associated with production of false identification cards).[6] *7

[6] The Court further notes that the defendant in Stabile actually suggested the use of forensic software, similar to that which was employed in this case, to categorize and isolate file types on his hard drive as an alternative search methodology that would have better protected his Fourth Amendment interests. United States v. Stabile, 633 F.3d 219, 240 n.13 (3d Cir. 2011).

Although the FTK software scanned Perez's computer hard drive and thumbdrives in their entirety to identify and segregate the requested files, the Court finds that this examination was permissible "to ensure that file names ha[d] not been manipulated to conceal their contents." Stabile, 633 F.3d at 241; see Mann, 592 F.3d at 782 (noting difficulties in locating image files); United States v. Hill, 459 F.3d 966, 978 (9th Cir. 2006) ("[I]mages can be hidden in all manner of files, even word processing documents and spreadsheets. Criminals will do all they can to conceal contraband, including the simple expedient of changing the names and extensions of files to disguise their content from the casual observer."). Thus, the Government's use of the FTK software to extract particular files for further review did not violate the Fourth Amendment.

ii. The Case Agents' Search of Extracted Files

Perez next argues that the "[o]pening [of] files in order to determine their contents" by the case agents constituted a general rummaging in violation of the Fourth Amendment. The Court rejects this argument. Although, the Court is mindful of the risks associated with searches of electronic data, and agrees that a warrant to search a computer for specific evidence is not "carte blanche to search every file on the hard drive," Stabile, 633 F.3d at 237, "the essential watchword of the Fourth Amendment is reasonableness," United States v. Skow, No. 11-373, 2013 WL 5493308, at *7 (N.D. Ga. Oct. 2, 2013). The Court concludes that the Government's search of Perez's computer and thumbdrives was reasonable under the Fourth Amendment.

First, the search warrant did not limit the Government's search to particular file types, but rather broadly authorized the search for and seizure of evidence related to the possession and *8 distribution of child pornography.[7] In light of this broad authorization, and "the particular difficulties in attempting to locate image files" on a computer, it was reasonable for the case agents to examine an array of file types, including the graphic, video, internet, and Ares files, which were the focus of their search. Stabile, 633 F.3d at 239 (citing Mann, 592 F.3d at 781)); cf. United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999) (seizure of child pornography images in closed files not authorized where warrant permitted only the search of the computer files for "names, telephone numbers, ledgers, receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances").

[7] The warrant authorized, inter alia, the search for and seizure of "[a]ll visual depictions of minors engaged in sexually explicit conduct (as defined in 18 U.S.C. § 2256) produced using minors engaged in such conduct, on whatever medium (e.g., digital media . . . ."; and all "correspondence, records, opened or unopened e-mails, chat logs, and

internet history, pertaining to the possession, receipt, access to or distribution of child pornography." (Def.'s Mot. to Suppress, Ex. A, 2.)

Second, courts have upheld as reasonable more probing computer searches than the search at issue in this case. In particular, several circuit and district courts have upheld computer searches where law enforcement officials conducted a cursory review of every file on the computer by opening it or previewing it to determine each file's contents. See United States v. Williams, 592 F.3d 511, 521 (4th Cir. 2010) (where warrant authorized search of defendant's computer and digital media for evidence related to computer harassment and threats, "the warrant impliedly authorized officers to open each file on the computer and view its contents, at least cursorily, to determine whether the file fell within the scope of the warrant's authorization"); United States v. Brown, No. 12-0367, 2013 WL 5508676, at *6 (E.D. Pa. Oct. 4, 2013); United States v. Fumo, No 06-319, 2007 WL 3232112, at *6 (E.D. Pa. Oct. 30, 2007); see also Burgess, 576 F.3d at 1094 ("[T]here may be no practical
9 substitute for actually looking in *9 many (perhaps all) folders and sometimes at the documents contained within those folders . . . It is particularly true with image files.").

In contrast to the above-cited cases, the record reveals that, in this case, the case agents previewed and/or opened a limited, filtered set of extracted files to determine whether they contained evidence of child pornography. Only the extracted graphic, video, and internet files in addition to those files related to the Ares application, were provided to the case agent for substantive review. At that point, the case agents viewed graphic images in a thumbnail version, and only opened them when it was believed that they contained evidence related to child pornography. They opened and played short portions of video files to determine whether they contained evidence related to the possession or distribution of child pornography as no thumbnail version was available; opened emails without attachments only if the subject line or sender gave them reason to believe that they contained evidence of child pornography; and opened and cursorily examined other extracted file types, e.g. internet history, to determine whether those files contained evidence that fell within the scope of the warrant and to identify the internet user at particular times. (Hearing Tr., May 1, 2015, 31-33, 45.) The record is devoid of evidence that at any point, the Government searched for evidence other than that which was authorized pursuant to the terms of the warrant. To the contrary, the previewing and/or opening of various files by the case agents was tailored to identifying evidence of child pornography, which was ultimately discovered, and which Perez's Motion seeks to suppress. See United States v. Richards, 659 F.3d 527, 540 (6th Cir. 2011) ("[S]o long as the computer search is limited to a search for evidence explicitly authorized in the warrant, it is reasonable for the executing officers to open the various types of files located in the computer's hard drive in
10 order to determine whether they contain such evidence."). *10

Finally, Perez has not presented any alternative search methodology that would have better "protect[ed] his legitimate interests and also permit[ted] a thorough search for evidence" of child pornography. Burgess, 576 F.3d at 1095 ("[Defendant] complains the particular methodology used in this case was overbroad, yet he offers no alternative methodology that would protect his legitimate interests and also permit a thorough search for evidence of drug trafficking."); see also Stabile, 633 F.3d at 240 (defendant "fails to propose a legitimate alternative methodology"). For all these reasons, the Court concludes that the Government's search was reasonable.

V. CONCLUSION

For the foregoing reasons, Perez's Motion to Suppress Physical Evidence is denied. An appropriate order follows.