

United States Court of Appeals For the First Circuit

No. 09-2252

UNITED STATES OF AMERICA,

Appellant,

v.

FERNANDO CRESPO-RÍOS,

Defendant, Appellee.

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF PUERTO RICO

[Hon. Jay A. García-Gregory, U.S. District Judge]

Before

Lynch, Chief Judge,
Torruella and Stahl, Circuit Judges.

J. Campbell Barker, Attorney, Appellate Section, Criminal Division, U.S. Department of Justice, with whom Lanny A. Breuer, Assistant Attorney General, Greg D. Andres, Acting Deputy Assistant Attorney General, Rosa Emilia Rodríguez-Vélez, United States Attorney, Nelson Pérez-Sosa, Assistant United States Attorney, Chief, Appellate Division, and Richard M. Re, Attorney, Criminal Division, U.S. Department of Justice, were on brief for appellant. Rachel Brill, for appellee.

June 8, 2011

("Crespo") was charged with (1) transferring obscene material to a minor under the age of sixteen in violation of 18 U.S.C. § 1470 and (2) possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B). The district court granted his motion to suppress the child pornography that agents discovered on various digital media while they were executing a warrant to search for evidence of (1) transferring obscene material to a minor in violation of 18 U.S.C. § 1470 and (2) enticing or coercing a minor in violation of 18 U.S.C. § 2422(b). The government now appeals the grant of the motion to suppress and the denial of its motion for reconsideration. We reverse and remand with instructions to deny the motion to suppress.

I. Background

In August 2007, Special Agent Odette D. Tavares of the Federal Bureau of Investigation entered a Spanish-language chat room posing as a twelve-year-old Puerto Rican girl. She was part of a covert online investigation aimed at identifying individuals attempting to engage in sexual relations with minors. An individual later identified as Crespo approached Tavares in the chat room and asked if Tavares had "MSN," referring to an instant messaging program. Tavares replied affirmatively, and they continued to chat through MSN's "instant messenger."

During this first conversation and others that followed over the course of approximately the next eight months, Crespo repeatedly communicated with Tavares about matters of a sexual nature despite being informed that she was only twelve years old and in seventh grade. During the majority of Crespo's chat sessions with Tavares, he displayed his bare erect penis to Tavares at some point. Crespo also repeatedly asked Tavares to meet with him and discussed the sexual activities that would take place if they met. He said, among other things, that (1) he would perform oral sex on Tavares, (2) he and Tavares could watch pornographic films before having sex, (3) the pair would have sex, (4) he would teach Tavares how to kiss and how to bathe him, and (5) she could model a g-string for him. Crespo also displayed two photos of himself to Tavares and repeatedly asked her to send him photos of herself.

In addition, Crespo mentioned or suggested at various points that he had engaged in sexual activities with minors before. During one chat, he noted that he had had sex with a fourteen-year-old girl. During another conversation, in the context of encouraging Tavares to shave her genital area, he told her that he knew of an individual who shaved her genital area as of the age of eleven.

Based on information learned as a result of the chats with Crespo, information received from the Puerto Rico Telephone

Company, and information gleaned from motor vehicle checks, Tavares submitted an affidavit in support of a search warrant. A magistrate judge issued a search warrant for a residence in Mayagüez, Puerto Rico. The warrant authorized agents to search the residence for evidence, fruits, and instrumentalities of a violation of 18 U.S.C. § 1470 (transfer of obscene material to a minor) and 18 U.S.C. § 2422(b) (coercion or enticement of a minor). The warrant incorporated "Attachment B" of Tavares's affidavit, which listed, among other items that could be seized, the following:

2. Records, documents, correspondence (limited to electronic communications), notes and/or any other materials relating to correspondence or contact between [Crespo] and [Tavares], including but not limited to electronic mail, chat logs, and electronic messages.

3. Records, documents, correspondence (including but not limited to electronic communications), notes, and/or any other materials relating to correspondence or contact between [Crespo] and individuals purporting to be minors, or any attempt by [Crespo] to induce any minor to engage in illegal sexual[] activity, including but not limited to electronic mail, chat logs, and electronic messages.

. . . .

10. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R[s], CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers,

electronic notebooks, cellular telephones, and personal digital assistants[.]

. . . .

12. Any computer equipment used to encode or store data

The main text of Tavares's affidavit referred to child pornography when it described the parameters of the potential search as including, among other things, "any and all chat logs, child pornography, child erotica, information pertaining to the sexual interest in children, [and] images depicting sexual contact between adults and minors." "Attachment B" authorized agents to search for "[c]orrespondence . . . which refers to . . . child pornography" and "sex toys to include but not limited to pornographic videos."

When Tavares executed the search warrant, she seized, among other things, a computer system, an external hard drive, and a number of CDs. The government forensically analyzed the seized items and discovered child pornography. The record is not clear as to exactly where and how each item of child pornography was discovered, or which items were photographs as opposed to videos.¹ According to Crespo's appellate brief, however, some of the child pornography was found on the external digital media. At oral argument, Crespo's counsel explained that child pornography images were found on both the computer Crespo used for his chats and on

¹ The magistrate judge did not conduct an evidentiary hearing because she concluded that the defendant's motion to suppress did not require one.

the external hard drive. Crespo's counsel also mentioned, in responding to a question about the location of the child pornography, that there was a video that was found on the external hard drive and also on a CD.

Crespo was ultimately charged with (1) knowingly possessing both still images and movie files of actual minors engaging in sexually explicit conduct, in violation of 18 U.S.C. § 2252, and (2) attempting to transfer obscene matters to someone who was apparently under the age of sixteen, in violation of 18 U.S.C. § 1470. Following his indictment, Crespo filed a motion to suppress the child pornography evidence on the ground that the search warrant was impermissibly general and authorized government agents to search for items without probable cause to believe those items would be present.²

A magistrate judge recommended that the court deny Crespo's motion to suppress, concluding that there was probable cause to search for child pornography. The magistrate judge also noted that the good faith exception to the exclusionary rule, see United States v. Leon, 468 U.S. 897 (1984), applied, and that the doctrine of inevitable discovery, see Nix v. Williams, 467 U.S. 431 (1984), might apply.

² As the government noted in its response in opposition to the motion to suppress, Crespo failed to state specifically which items he sought to suppress.

The district court rejected the magistrate's recommendation, concluding that Tavares's affidavit did not provide probable cause to believe that Crespo's digital media would contain child pornography. The district court also concluded that the good faith exception to the exclusionary rule did not apply. Addressing the magistrate's inevitable discovery argument, the district court noted that it believed that the plain view doctrine would be a more appropriate framework than the inevitable discovery doctrine, and concluded that the government ultimately could not prevail under the plain view doctrine. In a later order denying the government's motion for reconsideration, the district court clarified its reasoning on this point. According to the second order, because there was no probable cause to search for child pornography, the law enforcement officers who conducted a forensic examination of Crespo's digital media were not conducting a lawful search, and thus were not entitled to avail themselves of the plain view exception to the warrant requirement. The government now appeals.

II. Standard of Review

In assessing a district court's decision to grant a motion to suppress, "[w]e review 'the court's findings of fact for clear error and the application of the law to those facts de novo.'" United States v. Siciliano, 578 F.3d 61, 67 (1st Cir. 2009) (quoting United States v. Vilches-Navarrete, 523 F.3d 1, 12 (1st Cir. 2008)).

III. Discussion

The government makes three alternative arguments: (1) probable cause supported the warrant's authorization to search Crespo's computer for child pornography, (2) suppression was inappropriate given the good faith doctrine because the agents acted in objectively reasonable reliance on the warrant, and (3) the child pornography evidence should not be suppressed because it was discovered in plain view during a lawful search. Crespo responds, first, that there was no probable cause to seize and search all of Crespo's digital media in order to look for child pornography because Tavares's affidavit did not allege any nexus between Crespo's behavior and possession of child pornography and because the warrant application was overly broad. In addition, Crespo contends that the good faith exception is inapplicable because Tavares, who executed the warrant, could not have reasonably believed that there was probable cause to search for child pornography. Finally, Crespo argues that the plain view exception does not apply because the government had no probable cause to search the external hard drive or CDs at all.

We need not decide whether there was probable cause to search any of Crespo's digital media for child pornography because we resolve this appeal based on the inevitable discovery doctrine.³

³ The government did not expressly advance an argument under the inevitable discovery doctrine on appeal, and it is unclear whether it did so below. However, the magistrate judge addressed the

Under the inevitable discovery doctrine, "evidence that 'would inevitably have been discovered without reference to the police error or misconduct' may be admitted at trial." United States v. Hughes, No. 09-1646, 2011 WL 1332061, at *11 (1st Cir. Apr. 8, 2011) (quoting Williams, 467 U.S. at 448). "Such evidence is admissible 'so long as (i) the lawful means of its discovery are independent and would necessarily have been employed, (ii) discovery by that means is in fact inevitable, and (iii) application of the doctrine in a particular case will not sully the prophylaxis of the Fourth Amendment.'" Id. (quoting United States v. Zapata, 18 F.3d 971, 978 (1st Cir. 1994)).

In addressing the first prong of the inevitable discovery standard, we divide our analysis in order to explain why agents could have lawfully searched (1) Crespo's computer, (2) the external hard drive, and (3) the CDs, provided they were searching those digital media for certain categories of evidence. As explained below, these searches would have been lawful because

inevitable discovery doctrine, and Crespo therefore had the opportunity to argue that it was inapplicable. The inevitable discovery doctrine we employ here is similar in reasoning to the government's plain view argument, and it is clear that whether or not computer files fall under the plain view doctrine, "the independent source and inevitable discovery doctrines apply to the contents of the files." United States v. Stabile, 633 F.3d 219, 237 (3d Cir. 2011). We may exercise some latitude as to our grounds of decision where related doctrines are at issue. See, e.g., United States v. Sánchez, 612 F.3d 1 (1st Cir. 2010) (utilizing plain view doctrine rather than community caretaker doctrine).

there was probable cause to believe that at least some of the evidence listed in the warrant application's "Attachment B" would have been found on these digital media. Probable cause exists when, "given all the circumstances set forth in the affidavit[,] . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." United States v. Hicks, 575 F.3d 130, 136 (1st Cir. 2009) (quoting United States v. Feliz, 182 F.3d 82, 86 (1st Cir. 1999) (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983))) (internal quotation marks omitted).

There was certainly probable cause to believe that "records, documents, [and electronic] correspondence . . . relating to correspondence or contact between" Crespo and Tavares -- the second category of evidence in "Attachment B" -- would be found on Crespo's computer, because the affidavit included extensive documentation of online chats between Crespo and Tavares. This conclusion is not disputed. Thus, agents' search of Crespo's computer for this evidence would have been lawful.

The matter of the external hard drive is slightly more complicated because, according to Crespo's counsel's statements at oral argument, the hard drive had not been accessed in four years at the time of the search. Even crediting this statement as true, however, there was still probable cause to believe that evidence of similar interactions with other minors or purported minors -- the third category of evidence listed in "Attachment B" -- would be on

the external hard drive. This is so because Crespo had told Tavares that he had had sex with a fourteen-year-old girl and mentioned knowing someone who had shaved her genital area as of the age of eleven. Furthermore, Crespo cannot argue that records of these conversations would not constitute evidence of the crime charged because such records, if found, could be used to prove Crespo's intent. See United States v. Wolford, 386 F. App'x 479, 484 (5th Cir. 2010) (chat transcripts with anonymous parties found on defendant's computer admissible during trial for enticement of a minor to show motive and intent); United States v. Chase, 367 F. App'x 979, 982 (11th Cir. 2010) (transcript of chat in which defendant described molestation of a child admissible to show intent to entice a minor); United States v. McDarrah, 351 F. App'x 558, 563 (2d Cir. 2009) ("other act" evidence admissible during trial for attempted enticement because it was relevant to knowledge and intent and could be used to show that conduct was not a mistake or accident). Thus, the warrant here also properly authorized agents to search the external hard drive for, at the very least, evidence related to Crespo's contacts with other minors or purported minors. Similarly, even assuming that the searched CDs had also not been accessed for a number of years, there was probable cause to believe that, at the very least, evidence of these older communications would be on the CDs.

Regarding the second prong, we conclude that in the course of searching Crespo's computer for evidence of his interactions with Tavares and searching the external hard drive and CDs for evidence of similar interactions with other individuals, government agents would have inevitably discovered the child pornography. When searching digital media for "chats" and other evidence of enticement, government agents cannot simply search certain folders or types of files for keywords.⁴ First, like paper files, digital files may be mislabeled. See, e.g., United States v. Highbarger, 380 F. App'x 127, 130 (3d Cir. 2010) ("Suspects can easily hide information by mislabeling files, and, therefore, law enforcement officials are not required to accept a suspect's designation of what is contained in a particular file."); United States v. Williams, 592 F.3d 511, 522 (4th Cir. 2010) ("Surely, the owner of a computer, who is engaged in criminal conduct on that computer, will not label his files to indicate their criminality."); United States v. Hill, 459 F.3d 966, 978 (9th Cir. 2006) ("Forcing police to limit their searches to files that the suspect has labeled in a particular way would be much like saying police may not seize a plastic bag containing a powdery white substance if it is labeled 'flour' or 'talcum powder.'" (quoting United States v. Hill, 322 F. Supp. 2d 1081, 1090 (C.D. Cal.

⁴ Although there may be limitations on how government agents may search digital media in a case like this one, we need not address those limitations here.

2004))) . The suffixes or extensions of file names, which generally indicate file types, may be manipulated to disguise the true file types. See Hill, 322 F. Supp. 2d at 1090 ("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."); United States v. Harding, 273 F. Supp. 2d 411, 424 (S.D.N.Y. 2003) ("Files containing graphical images may be assigned file extensions, including 'TXT', that typically are assigned to text files. Files containing text may be assigned file extensions, including 'JPG' or 'GIF', that typically are given to graphical image files."); United States v. Gray, 78 F. Supp. 2d 524, 529 (E.D. Va. 1999) ("While the '.jpg' suffix generally denotes a picture file, there is no requirement that it do so, and, as a result[,] [the agent] could not be certain that files with the '.jpg' suffix did not contain the materials for which he was authorized to search."). Furthermore, a chat transcript, which begins as text, could be converted into an image and saved as an image file. See Harding, 273 F. Supp. 2d at 424 ("Text files . . . are readily scanned and converted into graphical image files."). Thus, in searching for evidence of Crespo's interactions with Tavares and other purported minors, forensic experts would have thoroughly combed through files and would have

inevitably discovered the child pornography that Crespo now seeks to suppress.⁵

Finally, "bear[ing] . . . in mind the social costs of the exclusionary rule," United States v. Scott, 270 F.3d 30, 45 (1st Cir. 2001), we consider the final prong of the inevitable discovery test. We conclude that the application of the doctrine here will not "provide an incentive for police misconduct or significantly weaken fourth amendment protection." United States v. Silvestri, 787 F.2d 736, 744 (1st Cir. 1986).⁶

⁵ The district court acknowledged as much in its opinion and order responding to the government's motion for reconsideration when, in its discussion of the plain view exception to the warrant requirement, it noted that if agents had not been searching for child pornography, "the alleged child pornography found in Defendant's digital media would have been seized pursuant to a search for evidence of enticement and transfer of obscene material to a minor."

⁶ Crespo also argues that we should dismiss this appeal because the United States Attorney did not personally certify, pursuant to 18 U.S.C. § 3731, that the appeal was not taken for the purpose of delay and that the evidence suppressed is substantial proof of a material fact. Instead, an Assistant United States Attorney ("AUSA") electronically signed the required notice of appeal after consulting with the United States Attorney, who verified that the requirements of § 3731 were met.

We reject Crespo's argument. Given the process here -- which included review by the United States Attorney and then by the Solicitor General -- and the fact that the statute itself notes that its "provisions shall be liberally construed to effectuate its purposes," 18 U.S.C. § 3731, we conclude that the AUSA's submission of the notice of appeal satisfies the statute. See United States v. Lazar, 604 F.3d 230, 242 n.11 (6th Cir. 2010) ("As to defendant's contention that certification signed by an AUSA . . . -- as opposed to the United States Attorney -- cannot satisfy § 3731, we reject such a requirement, especially in light of the review process outlined above [i.e., the process in which the

IV. Conclusion

For the reasons stated, we reverse the district court's order and remand with instructions to deny the motion to suppress.

Reversed and Remanded.

Solicitor General makes a final decision about whether to appeal]."); United States v. Wolk, 466 F.2d 1143, 1146 n.2 (8th Cir. 1972) ("While [18 U.S.C. § 3731] refers to the 'United States attorney[,] the appellee cites no cases nor suggests any compelling reasons which justify a decision that would so needlessly circumscribe the ability of the United States Attorney to delegate responsibility. We recognize that the statute is to be 'liberally construed to effectuate its purposes', 18 U.S.C. § 3731, and[] we can unearth no reason to disregard that direction in this case.").