FILED
United States Court of Appeals
Tenth Circuit

May 13, 2019

Elisabeth A. Shumaker
Clerk of Court

PUBLISH

UNITED STATES COURT OF APPEALS

FOR THE TENTH CIRCUIT

UNITED STATES OF AMERICA

Plaintiff - Appellee,

v.

JASON LOERA,

Defendant - Appellant.

No. 17-2180

Appeal from the United States District Court
for the District of New Mexico
(D.C. No. 1:13-CR-01876-JB-1)

Jerry A. Walz, Walz and Associates, P.C., Albuquerque, New Mexico for Defendant-Appellant.

Kristopher N. Houghton, Assistant United States Attorney (John C. Anderson, United States Attorney, with him on the brief), Albuquerque, New Mexico for Plaintiff-Appellee.

Before **LUCERO**, **EBEL**, and **PHILLIPS**, Circuit Judges.

EBEL, Circuit Judge.

This appeal requires us to apply Fourth Amendment principles to a situation where a police officer executing a warrant to search an electronic storage device for evidence of one crime discovers evidence of other criminal activity. Here, while

executing a warrant to search Jason Loera's home for evidence of computer fraud, FBI agents discovered child pornography on four of Loera's CDs. Despite discovering the pornography, the agents continued their search for evidence of computer fraud—one agent continued to search the CDs that were found to contain some child pornography and a second agent searched other electronic devices belonging to Loera, not including those particular CDs (Search 1). After the agents finished their on-site search, they seized a number of electronic devices that appeared to contain evidence of computer fraud, plus the four CDs that were found to contain child pornography, and then brought the seized items back to their office. One week later, one of the agents reopened the CDs that he knew contained some child pornography so that he could describe a few pornographic images in an affidavit requesting a (second) warrant to search all of the seized electronic devices for child pornography (Search 2). A magistrate judge issued the warrant, and, upon executing it through two searches, the agents found more child pornography.

In the subsequent prosecution against him for possessing child pornography, Loera filed a motion to suppress the evidence seized pursuant to each search, arguing that the searches violated the Fourth Amendment. On denial of his motion, Loera pled guilty to receipt of child pornography but preserved his right to appeal that denial. Exercising jurisdiction under 28 U.S.C. § 1291, we affirm the denial of Loera's motion to suppress. We hold, among other things, that the Fourth Amendment does not require police officers to stop executing an electronic search warrant when they discover evidence of an ongoing crime outside the scope of the

warrant, so long as their search remains directed at uncovering evidence specified in that warrant.

I. BACKGROUND

This case involves several police searches governed by the Fourth Amendment. The Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. Generally, for a search to be reasonable, it must be authorized by a warrant that "particularly" describes "the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. Once officers obtain a sufficiently particular warrant, they must execute it according to the warrant's terms. Horton v. California, 496 U.S. 128, 140 (1990). The following undisputed facts explain how the warrant-based searches in this case arose.

In 2012, the FBI began investigating Jason Loera for illegally intercepting e-mails intended for then-sitting New Mexico Governor Susana Martinez and her staff in violation of 18 U.S.C. § 2511 (illegal interception) and 18 U.S.C. § 1030 (computer fraud) [collectively, "computer fraud"]. As part of that investigation (more details of which can be found in the district court's opinion United States v. Loera, 59 F. Supp. 3d 1089, 1095–1108 (D.N.M. 2014)), FBI agents applied for and received a warrant to search Loera's residence for computer fraud, including any such evidence residing on electronic devices or storage media ("the first warrant").

The first warrant authorized FBI agents to search and seize, in relevant part, "All records, in any form, relating to violations of [computer fraud], involving Jason

Loera." ROA Vol. I at 37. The warrant defined the terms "records" and "information" as including: "all of the foregoing items of evidence in whatever forms and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data)." Id. at 39. In a separate provision, the warrant sought "Any computers, cell phones, and/or electronic media that could have been used as a means to commit the offenses described on the warrant." Id. at 87. Finally, for any electronic device, whether it was used to commit the offenses or simply had relevant records stored on it, the warrant permitted the agents to search and seize evidence of who used, owned, or controlled the device, such as "configuration files . . . documents, browsing history . . . photographs, and correspondence . . . ." Id. at 38.

A. The First Search

On November 20, 2012, FBI agents including Agent Aaron Cravens and Special Agent Brian Nishida executed the first search warrant. They discovered a large volume of electronic media in Loera's residence, including CDs, DVDs, laptop computers, external hard drives, a USB flash drive, an iPhone, and an iPad. Cravens and Nishida were responsible for "previewing" the CDs at Loera's residence to ensure that the FBI seized only those CDs that contained information relevant to the authorized investigation. ROA Vol. II at 53, 58. The two agents split up the CDs between themselves and searched them separately.

Cravens tried to view the files of the first CD using a program called FTK Imager, which would have allowed Cravens to limit his search to a particular type of

file, for example, only image, text, or audio files. However, the program did not work. Consequently, Cravens opened the CD on a computer and used the "thumbnail view" to preview the files stored on it, meaning, he saw small images of the files, the file names, and the file types in a vertical list that he had to scroll through to see in its entirety. Although Cravens believed he had authority under the first warrant to view the entire contents of the CD, Cravens used the thumbnail-image view to fast-track his search. He would scroll past irrelevant files but "click[] on anything that didn't appear correct, or any documents" to open them. Id. at 92. While Cravens was "scrolling down through the images or files . . . on the CDs, [he] found what looked like a nude child." Id. at 60. He opened the file to confirm that it was an image of child pornography. After determining that it was, Cravens ejected the CD from his computer, set it aside, and alerted Agent Nishida and the FBI agent in charge of Loera's case. Then, Cravens searched the rest of the CDs assigned to him for evidence of computer fraud. Cravens later found a child pornography image on a second CD. Just as he did with the first, Cravens set the CD aside after discovering the illegal images and did not open any other files on that CD.

Agent Nishida took a different approach to his search. He previewed the files on his assigned CDs using the "details view" of Windows Explorer, meaning that he saw a list of files, file names, and last-modified dates of those files, but not pictures associated with the files. Id. at 157. For his search of the CDs, or "triage," as he called it, Nishida would open two or three files on each CD and then determine from that sample whether the CD should be seized pursuant to the warrant. Id. at 160. If Nishida

found something he believed might be responsive to the warrant in the files that he sampled, he would set the CD aside to be reviewed off-site. As he was sampling files, Nishida found child pornography on two CDs. Unlike Cravens, Nishida did not cease his search of those CDs after discovering child pornography; he continued sampling files on the CDs to determine if they contained information that was responsive to the warrant.

The FBI seized thirteen CDs in total from Loera's residence: four contained child pornography images and nine contained evidence of computer fraud.[1] In addition to the thirteen CDs, the FBI seized computers, external hard drives, an iPhone, and an iPad.

B. The Second Search

One week later, on November 27, 2012, Cravens decided to apply for a search warrant to search the items seized from Loera's residence for child pornography. Cravens wanted to include in his warrant affidavit a detailed description of one child pornography image from each of the four CDs on which he and Nishida had found child pornography during their on-site preview. Consequently, Cravens opened each of the four CDs, viewing several images on each, to find child pornography images that he could accurately describe. Viewing the photos and drafting the affidavit took a total of two-and-a-half hours. However, Cravens testified before the district court that he did not spend "anywhere near the two-and-a-half hours" actually looking at photos on the CDs. Id. at 74-75.

[1] There is no indication in the record whether the four CDs that contained child pornography also contained evidence responsive to the warrant. However, Loera does not challenge the FBI's seizure of those CDs pursuant to the first warrant.

Cravens' affidavit included two sections. In Section I, Cravens described his training and experience with computers and child pornography. In Section II, Cravens explained the details of the FBI's investigation of Loera that led to the agent's discovery of child pornography on the CDs in Loera's residence. In particular, paragraph 21 described in general terms how Cravens discovered the child pornography:

> 21. In the process of executing this warrant, an FBI certified computer forensic examiner and a computer analysis response team (CART) technician previewed the loose media located during the search (*e.g.*, thumb drives, CD-Rs, DVD-Rs, memory cards, etc.) for evidence relevant to the original unrelated investigation. During the preview, the examiners identified four writable CDs which appeared to contain images of child pornography. The CDs were seized and placed in the evidence control room at the local FBI office.

ROA Vol. I at 120. In paragraph 23, Cravens explained that on November 27, 2012, he "reviewed the four CDs . . . that were believed to contain child pornography," id. at 121, and that "[d]uring the review of the CDs, [he] observed multiple pictures of children many of which are in various states of dress," id. Then, in paragraphs 24-27, Cravens provided a detailed description of one image from each CD that depicted a minor engaged in sexually explicit conduct. Cravens' descriptions included the apparent age of the minor and the conduct depicted. On November 29, 2012, based on Cravens' affidavit, a federal magistrate judge approved a warrant to search the thirteen CDs and six other electronic devices that were seized from Loera's residence for child pornography ("the second warrant").

C. Searches Pursuant to the Second Warrant

Agent Nishida executed the second warrant on two separate dates. In December 2012, Nishida searched Loera's laptop pursuant to both the first and second warrants, looking for evidence of computer fraud and child pornography. He discovered more than 730 child pornography images on Loera's laptop. In April 2013, Nishida searched the four CDs seized from Loera's residence for child pornography pursuant to the second warrant. He discovered approximately 330 images and two movies of child pornography on those CDs.

D. Proceedings Below

A federal grand jury indicted Loera on several counts of possessing child pornography that implicated the images found on both his laptop and his CDs. Loera filed a motion to suppress that child pornography evidence, and the district court denied the motion. Loera filed a motion for reconsideration, which the district court also denied. Following that denial, Loera pled guilty to one count of knowingly receiving child pornography in violation of 18 U.S.C. §§ 2252(a)(2), 2252(b)(1), and 2256, pursuant to a plea agreement, but he reserved the right to appeal the denial of his motions.

On appeal, Loera argues that the district court should have suppressed the child pornography evidence discovered during the first search, the second search, and the searches conducted pursuant to the second warrant because, according to Loera, each search was unlawful. Loera argues that the first search exceeded the scope of the first warrant, the second search exceeded the scope of the first warrant, and the

last two searches, while authorized by the second warrant, were unlawful because that warrant was invalid. Additionally, Loera maintains that none of the exceptions to the warrant requirement apply to the searches in this case. We conclude that the first search was lawful, but we agree with Loera that the remaining searches were unlawful. Nevertheless, we AFFIRM the district court's denial of Loera's motion to suppress and motion to reconsider under the inevitable discovery doctrine.

II. DISCUSSION

A. Standard of Review

"When reviewing the district court's denial of a motion to suppress, we view the evidence in the light most favorable to the government and accept the district court's factual findings unless they are clearly erroneous," United States v. Grimmett, 439 F.3d 1263, 1268 (10th Cir. 2006), but "[t]he ultimate question of reasonableness under the Fourth Amendment is a legal conclusion that we review de novo." Id. Accordingly, de novo review applies to the issues we address in this opinion, including, the scope of a search warrant, United States v. Angelos, 433 F.3d 738, 745 (10th Cir. 2006), the sufficiency of a search warrant, United States v. Danhauer, 229 F.3d 1002, 1005 (10th Cir. 2000), the applicability of the good-faith exception, id., and the applicability of the inevitable discovery doctrine, United States v. Christy, 739 F.3d 534, 540 (10th Cir. 2014).

B. Validity of the Government's Application for the First Warrant

First, Loera argues that the FBI agents obtained the initial warrant to search his residence for evidence of computer fraud as a pretext to search instead for

evidence of child pornography. The district court disagreed, finding that the sole purpose of the first search was to uncover evidence of computer fraud. We affirm that conclusion.

Loera's pretext argument is based on a statement that Agent Nishida made in a report dated February 28, 2013, three months after the first and second searches were conducted. In that report, Nishida wrote:

> On November 14, 2012, SA Michael Boady requested that the above listed specimen or specimens be examined for evidence of intercepting a communication. For example, e-mail messages to or from the domain Susanna2010.com. In addition, SA Boady requested that the evidence also be examined for evidence of child pornography possession and receipt.

ROA Vol. II at 191–92. Loera argues that this report proves that on November 14, 2012, six days before the first search, Agent Nishida received instructions to search Loera's home and effects for evidence of child pornography.

The district court made explicit factual findings to the contrary, which are supported by the record. First, the district court found that, had the FBI agents had suspicions that Loera possessed child pornography, agents would have included that information in their application for the first warrant. Second, Agent Nishida testified at the suppression hearing that the February 2013 report summarized two separate instructions from SA Boady: on November 14, 2012, Boady instructed Nishida to search for evidence of interception, and, later, Boady instructed Nishida to search for evidence of child pornography. Finally, both Cravens and Nishida testified at the suppression hearing that the purpose of the November 20 search was only to uncover

evidence of computer fraud, and the district court credited that testimony. Each of these facts supports the district court's determination that the agents conducted the first search solely to look for evidence of computer fraud. And we are unpersuaded by Loera's only evidence of pretext, the report written three months after the allegedly pretextual search.[2]

Thus, we conclude the FBI agents had no pretextual motivations for obtaining the first warrant, and we affirm the district on this issue.

C. Reasonableness of the First and Second Searches

Next, we determine that the first search of Loera's residence was reasonable because it was directed solely at uncovering the items specified in the first warrant both before and after the officers discovered the child pornography evidence. However, we conclude that the second search was unreasonable because it was directed at uncovering evidence of child pornography.

1. Relevant legal principles

The Fourth Amendment provides:

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

[2] Alternatively, even if the agents had an additional motive for conducting the first search, that argument would fail as a matter of law under Whren v. United States, 517 U.S. 806, 813 (1996).

U.S. Const. amend. IV. It is now well-recognized that "the ultimate touchstone of the Fourth Amendment is 'reasonableness.'" Brigham City v. Stuart, 547 U.S. 398, 403 (2006). "[R]easonableness generally requires the obtaining of a judicial warrant," Riley v. California, 134 S.Ct. 2473, 2482 (2014), subject to only a few exceptions. The warrant must "particularly" describe "the place to be searched, and the persons or things to be seized," U.S. Const. amend. IV.

However, obtaining a sufficiently particular warrant is just the first step to conducting a reasonable search. The officers tasked with executing a sufficiently particular warrant must conduct their search "strictly within the bounds set by the warrant." Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics, 403 U.S. 388, 395 n.7 (1971) (quoting Marron, 275 U.S. at 196). The Supreme Court has held that, "[i]f the scope of [a] search exceeds that permitted by the terms of a validly issued warrant . . . the subsequent seizure [of evidence] is unconstitutional without more." Horton v. California, 496 U.S. 128, 140 (1990).

Determining whether a search exceeds the scope of its authorizing warrant is, like most inquiries under the Fourth Amendment, an exercise in reasonableness assessed on a case-by-case basis. Dalia v. United States, 441 U.S. 238, 258 (1979) (holding that the manner of a search is subject to "later judicial review as to its reasonableness"). The general Fourth Amendment rule is that investigators executing a warrant can look anywhere where evidence described in the warrant might conceivably be located. United States v. Ross, 456 U.S. 798, 824 (1982). For example:

> Just as probable cause to believe that a stolen lawnmower may be found in a garage will not support a warrant to search an upstairs bedroom, probable cause to believe that undocumented aliens are being transported in a van will not justify a warrantless search of a suitcase. Probable cause to believe that a container placed in the trunk of a taxi contains contraband or evidence does not justify a search of the entire cab.

Id. This limitation works well in the physical-search context to ensure that searches pursuant to warrants remain narrowly tailored, but it is less effective in the electronic-search context where searches confront what one commentator has called the "needle-in-a-haystack" problem. Orin S. Kerr, Digital Evidence and the New Criminal Procedure, 105 Colum. L. Rev. 279, 301 (2005). Given the enormous amount of data that computers can store and the infinite places within a computer that electronic evidence might conceivably be located, the traditional rule risks allowing unlimited electronic searches.

To deal with this problem, rather than focusing our analysis of the reasonableness of an electronic search on "what" a particular warrant permitted the government agents to search (i.e., "a computer" or "a hard drive"), we have focused on "how" the agents carried out the search, that is, the reasonableness of the search method the government employed. See United States v. Burgess, 576 F.3d 1078 (10th Cir. 2009); United States v. Walser, 275 F.3d 981 (10th Cir. 2001); United States v. Carey, 172 F.3d 1268 (10th Cir. 1999). Our electronic search precedents demonstrate a shift away from considering what digital location was searched and toward considering whether the forensic steps of the search process were reasonably directed at uncovering the evidence specified in the search warrant. Shifting our

focus in this way is necessary in the electronic search context because search warrants typically contain few—if any—restrictions on where within a computer or other electronic storage device the government is permitted to search. See United States v. Christie, 717 F.3d 1156, 1165 (10th Cir. 2013) (holding that, so long as an electronic search warrant requires the government to "direct all of its search efforts" toward evidence relating to a specific crime, the warrant is sufficiently particular, even where it permits the government to search a "computer" for "all records" relating to the crimes of "murder, neglect, and abuse"). Because it is "unrealistic to expect a warrant prospectively [to] restrict the scope of a search by directory, filename or extension or to attempt to structure search methods," Burgess, 576 F.3d at 1093 (alteration added), our ex post assessment of the propriety of a government search is essential to ensuring that the Fourth Amendment's protections are realized in this context. Our precedent of Carey, Burgess, and Walser, to which we turn next, are instructive as to what constitutes a reasonable electronic search pursuant to a valid warrant.

Carey is the only case in which we invalidated an electronic search for exceeding the scope of its authorizing warrant. See 172 F.3d at 1276. There, a police officer obtained a warrant to search files on the defendant's computer for evidence "pertaining to the sale and distribution of controlled substances." Id. at 1270. Prior to searching the computer, the officer first viewed the computer's file directory, which showed numerous "JPG" files with sexually suggestive titles. Id. During his search, the officer came across a number of files that he did not recognize

and that he was unable to view on the computer that he was using. Id. at 1271. To view the files, the officer downloaded them onto a separate disk, inserted that disk into another computer, and then was immediately able to view a "JPG file" that depicted child pornography. Id. Rather than navigating away from the nonresponsive material, the officer "downloaded approximately two hundred forty-four" more JPG files and then transferred them to nineteen disks, viewing five to seven images on each disk to determine that they all contained child pornography. Id. The whole process took about five hours. Id. at 1273. After he had catalogued the child pornography images in this manner, he then "returned" to his "original task of looking for evidence of drug transactions." Id. at 1271.

The Carey court held that this was an unlawful, general exploratory search because, although it was permissible for the officer to open the first JPG file to see if it was responsive to the warrant, id. at 1273 n.4, his opening of the remaining files exceeded the bounds of the authorizing warrant, id. at 1276. The Carey court's holding turned on four facts: (1) the officer spent five hours, a significant amount of time, specifically perusing the trove of nonresponsive material, id. at 1273; (2) the nonresponsive files were characteristically distinct and set apart from the other files on the computer (such that they could have been avoided) because each file was labeled "JPG," many had sexually suggestive titles, and the officer had to download them to open them, id. at 1274; (3) the officer did not discover the files inadvertently (at least after his first look), id. at 1273; and (4) a more narrowly tailored search was possible—the officer could have gone back to searching for drug-related documents

much sooner than he did, id. at 1273. Importantly, we did not condemn the officer's decision to return to searching for drug-related documents after discovering the child pornography, but, instead, we condemned his "temporar[y] abandon[ment]" of the original search to conduct a "five hour search of the child pornography files." Id. at 1273.

Next, we turn to Walser and Burgess, both of which upheld electronic searches in which the investigator discovered incriminating, nonresponsive material while executing a search warrant but then navigated away from it. In United States v. Walser, the police obtained a warrant to search the defendant's hotel room for electronically stored records of "evidence of the possession of controlled substances." 275 F.3d 981, 983–84 (10th Cir. 2001). A police officer searched the room pursuant to the warrant and found a laptop and a digital camera. Id. at 984. The agent seized the laptop, removed it from the hotel room, and then conducted a drug-specific search of the laptop, looking for "ledgers of drug transactions or images of drug use." Id. In order to find those things, the agent employed a particularized search method that "selectively proceeded to the 'Microsoft Works' sub-folder on the premise that[,] because Works is a spreadsheet program, that folder would be most likely to contain records relating to the business of drug trafficking." Id. at 986. It was while searching the contents of the Works folder that the officer came across a file labeled "bstfit.avi" and opened it. Id. at 984. When he viewed the contents, he discovered that the file contained child pornography images. Id. at 986–87. He then immediately ceased his search. Id.

We upheld the officer's search as reasonable because we determined that, by using a particularized search method, the officer avoided conducting the kind of "sweeping, comprehensive search of a computer's hard drive" that Carey prohibited. Id. at 986. The defendant in Walser argued that the agent exceeded the scope of the warrant by opening the "AVI file," a video file, because "it could not possibly have contained the type of evidence the [a]gent was authorized to search for, namely, records of drug transactions or still images of drug use." Id. at 987. We rejected that argument by interpreting Carey to excuse an officer's discovery of child pornography during a search for "relevant records in places where such records might logically be found" so long as the officer does not conduct a supervening search specifically directed at finding pornography evidence. Id. at 986. Applying that rule, we held in Walser that the officer's opening the "bstfit.avi" file was permissible because (1) he was looking in a folder that was "most likely to contain records relating to the business of drug trafficking" when he opened it, and (2) he did not conduct an intervening search directly focused on child pornography like the agent in Carey. Id. Based on those facts, we concluded that the "search was reasonable and within the parameters of the search warrant" and that the evidence found as a result of it did not need to be suppressed. Id. at 987.

Finally, in United States v. Burgess, 576 F.3d 1078 (10th Cir. 2009), we again upheld an electronic search that uncovered evidence of child pornography as reasonable and within the scope of its authorizing warrant. There, police obtained a warrant to search a motorhome for, among other things, "computer records" that

would tend to show "conspiracy to sell drugs." Id. at 1083. The warrant incorporated the affidavit on which it was based, which stated that the affiant "knows that persons involved in trafficking or the use of narcotics often keep photographs of coconspirators or photographs of illegal narcotics in their vehicle." Id.

Based on the warrant, officers searched two hard drives and a laptop found in the motorhome. Id. An agent searched one of the hard drives by using a program called EnCase, which copies the contents of a hard drive over to a computer to prevent file corruption. Id. at 1083–84. EnCase allows an investigator to "preview" reduced-sized photos of each image file as they are being copied. Id. at 1084, 1094. The agent took advantage of this feature and viewed each image file on the hard drive as it was being copied. Id. at 1084. After viewing 200-300 digital images, mostly personal photos, the agent saw an image that looked like child sexual exploitation. Id. He then closed the preview program and sought a warrant to search all of the defendant's electronic storage devices for evidence of child pornography. Id. Upon conducting that search, the agent found more than one hundred thousand illegal images. Id.

The defendant asked the district court to suppress the child pornography evidence because, he argued, the agent's use of the "preview" program exceeded the scope of the warrant because he did not employ a particularized search method like the agent in Walser but instead looked through each image file contained on the hard drive. We determined that the agent's use of the "preview" program was reasonable and did not exceed the scope of the warrant for two reasons. First, we noted that,

because the warrant did not expressly limit the file types that the agent was allowed to search, for example, by limiting the search to text files (.doc, .wpd, .txt, etc.), the agent was well within the scope of the warrant when he decided to view all of the image files on the hard drive using the preview program. Id. at 1092. Second, we determined that there was no reasonable way for the agent to conduct a more narrowly tailored search because, when the object of a search is likely to be an image file, as it was in Burgess, "there may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders." Id. at 1094.

Reading these cases together, we determine that four features of the unconstitutional search in Carey demonstrate that it was unreasonably directed at uncovering evidence of child pornography, rather than directed at the evidence specified in the warrant, and distinguish it from the reasonable searches in Walser and Burgess: (1) the length of time the searching officer spent looking at the incriminating, nonresponsive evidence (five hours in Carey versus less than one minute in Walser and Burgess); (2) the fact that the nonresponsive files were set apart from the responsive files saved on the storage device (JPG files downloaded onto separate disks in Carey versus generic files intermingled all in one place in Burgess); (3) the manner in which the evidence was discovered (purposefully in Carey versus inadvertently in Walser and Burgess);[3] and (4) the breadth of the search method

[3] We acknowledge that in Horton v. California, 496 U.S. 128, 130 (1990), the Supreme Court held that, in physical searches, "even though inadvertence is a

employed (the wide detour in Carey versus the narrowly tailored search in Walser). Contrary to Loera's assertion, these cases do not require that officers stop searching upon discovering evidence of a crime outside the scope of the warrant. Such a rule would prohibit what the Fourth Amendment expressly permits—reasonable searches based upon a warrant supported by probable cause. We have never required that.

This conclusion brings us in line with every circuit that has confronted this issue. See United States v. Stabile, 633 F.3d 219, 240 (3d Cir. 2011) (upholding denial of motion to suppress where officers continued warrant-authorized search of the defendant's computer for financial crimes after discovering child pornography); United States v. Williams, 592 F.3d 511, 521–24 (4th Cir. 2010) (upholding search where the officer continued his warrant-authorized search of the defendant's computer for evidence of "making threats and computer harassment" after discovering child pornography); United States v. Miranda, 325 F.App'x 858, 859–60 (11th Cir. 2009) (per curiam) (unpublished) (upholding search where officer continued his warrant-authorized search for evidence of counterfeit software after discovering child pornography); United States v. Wong, 334 F.3d 831, 834 (9th Cir.

---

characteristic of most legitimate 'plain view' seizures, it is not a necessary condition." However, because Carey, Walser, and Burgess, each of which succeeded Horton in time, considered the subjective intentions of the searching officers where that information was available, we continue to include inadvertence as a factor to consider when deciding whether an electronic search fell within the scope of its authorizing warrant or outside of it. The fundamental differences between electronic searches and physical searches, including the fact that electronic search warrants are less likely prospectively to restrict the scope of the search, justify our inclusion of that factor. See Horton, 496 U.S. at 139 (abandoning inadvertence as a necessary condition for a legitimate plain view seizure).

2003) (upholding denial of motion to suppress where the officer continued his warrant-authorized search of the defendant's computer for, among other things, "[a]ny maps, receipts, or writings, depicting Churchill County Nevada" after discovering child pornography).

Although officers do not have to stop executing a search warrant when they run across evidence outside the warrant's scope, they must nevertheless reasonably direct their search toward evidence specified in the warrant. What that looks like depends on the particular facts of a given case. Narrowly tailored search methods that begin looking "in the most obvious places and [then] progressively move from the obvious to the obscure," Burgess, 576 F.3d at 1094, should be used where possible but are not necessary in every case. In cases like this one, where the electronic storage device is not well-organized and the most practical way to search it is through an item-by-item review, "there may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders." Id. In such a case, however, the searching officer must respond appropriately to what he or she sees. The reasonableness of a search evolves as the search progresses and as the searching officer learns more about the files on the device that he or she is searching.

An analogy to the physical realm is helpful here. Imagine a warrant authorizes police officers to search a "residence" for evidence of "firearms and ammunition." Under that warrant, it would be reasonable for a police officer to search the medicine cabinet in the bathroom for a minute or two to see if a small gun or ammunition is

hidden there, however, it would be unreasonable for the officer to spend two hours reading the labels on each bottle of medicine in the cabinet. On the other hand, if the warrant had authorized the officer to search the residence for evidence of "illegal drug trafficking and manufacture," an intensive search of the medicine cabinet would be reasonable. In both cases, the medicine cabinet is fair game to search, but the intensity level of the permitted search differs depending on the evidence to be seized. The same is true for electronic searches. While in some cases many (perhaps all) electronic areas of a computer will be fair game to search, the level of intensity that officers are permitted to spend searching those areas will differ depending on whether the area appears to contain responsive material. This is true even when officers come across evidence of incriminating, nonresponsive material. In all cases, the ultimate test is the one mandated by the Fourth Amendment: whether the search was "reasonable" under the circumstances. In the case of a computer search, "reasonableness" requires officers to take into account the flexibility of computers and the multiple configurations to which they may be adapted. As the computer search continues and as the executing officer obtains more information about how a suspect used his computer, that too may inform the reasonableness of the continuing search.

We now apply these principles to the November 20 and 27 searches conducted in this case.

2. November 20 search was reasonable

Loera argues that, although the first warrant permitted the FBI agents to search his CDs for evidence of computer fraud, the officers' search exceeded the scope of the first warrant when they continued searching after discovering evidence of child pornography. We disagree. The searches that Agent Cravens and Agent Nishida each conducted of Loera's CDs on November 20 were reasonable and conducted within the scope of the first warrant because at all times each was reasonably directed at discovering evidence of computer fraud. Therefore, the first search did not violate the Fourth Amendment and thus did not warrant suppression of the evidence discovered during that search.

The agents' searches on November 20 resemble the searches in Walser and Burgess more than they resemble the search in Carey, both before and after they discovered the child pornography evidence. First, both agents here spent very little time looking at the child pornography images they discovered. They noticed them, alerted a supervisor, and then moved on to the rest of the images on the same CD (in Nishida's case), or the other CDs (in Cravens' case), looking for evidence of computer fraud. Both responses were reasonable because, as mentioned above, the agents were not required to stop searching altogether. And both responses demonstrate an effort to navigate away from the nonresponsive material and toward files that they believed were more likely to contain material responsive to the warrant. Second, the files on the CDs that the agents previewed were not characteristically distinct or set apart from the other files, in contrast to Carey. Agent Cravens testified that, when he put a CD into his computer to see the files that it

contained, the computer pulled up a generic list of those files. The record does not indicate that there were any folders or distinctive titles setting clearly apart the nonresponsive child pornography files from the other files on the disk. Loera bears the burden of proof on his suppression motion, and he has offered no evidence on this point. Third, the agents discovered the child pornography files inadvertently on November 20. Fourth, both agents' search methods were reasonably narrow under the circumstances, considering the fact that the CDs did not seem particularly organized. Given that the warrant permitted the agents to search the CDs for "photographs," "documents," and "configuration files," it was reasonable for Nishida and Cravens to search all file types on the CDs (image, video, and text) for evidence of computer fraud rather than to narrow that search to one particular file type. The agents' searches on November 20 were reasonable because they fell within the scope of the first warrant both before and after they discovered the child pornography evidence. We reverse the district court's ruling to the contrary.

3. November 27 search was unreasonable

Loera also argues that Agent Cravens' subsequent search on November 27, 2012, of the four seized CDs that contained child pornography violated the Fourth Amendment because Cravens was "[i]ntentionally searching for evidence of a crime outside the scope of the [f]irst [w]arrant prior to obtaining a new warrant." Aplt. Br. 29. In making this argument, Loera accepts that the first warrant permitted the government to seize the four CDs that were found to contain some child pornography and to search them for evidence of computer fraud. Therefore, Loera challenges Cravens' November 27

search only for exceeding that permission. Accordingly, we confine our analysis to whether the second search exceeded the scope of the first warrant. The district court concluded that it did and that neither exigent circumstances nor any other exception to the warrant requirement justified that search. We agree and conclude that the district court correctly excised the evidence obtained during the November 27th search from Cravens' affidavit for the second warrant. Several of the district court's factual findings support that result.

The district court found that "Cravens was not searching for evidence of electronic fraud" on November 27 but instead was searching for child pornography. Dist. Ct. Op. at 144. The district court based this finding on Cravens' testimony at the suppression hearing that he reopened Loera's CDs on November 27 specifically "[t]o write a description of an image on the disc" so that he could "obtain a second warrant for child pornography." ROA Vol. II at 72. That admission is the most probative fact in the record that Cravens' search was directed at finding child pornography. The district court also found that Cravens had the four CDs for a total of two-and-a-half hours that day, during which time he searched the CDs and drafted the second affidavit. Although the record does not indicate how long Cravens searched the CDs, he testified at the suppression hearing that he looked at several images on each CD—"more than just a couple" but "[m]ost likely less than a dozen." ROA Vol. II at 143. Whatever the amount of time, Cravens' devoted it exclusively to nonresponsive material. Rather than navigate away from the child pornography images when he found them, Cravens explicitly navigated toward such images. Based on these findings, we

agree with the district court that, in contrast with the agents' searches on November 20, Agent Cravens' search on November 27 was unreasonable because it was directed at uncovering evidence of child pornography.

The government argues that two exceptions save Cravens' search from violating the Fourth Amendment: the plain view doctrine and the foregone-conclusion exception. We disagree. For its plain view argument, the government asserts that the law permitted Agent Cravens to take a "second look" at the child pornography images on Loera's CDs because members of the FBI had already seen the images in plain view during a lawful search, and, therefore, his "second look" was no further invasion of Loera's privacy than the initial, lawful viewing. The government points to a Fourth Circuit case, United States v. Jackson, 131 F.3d 1105 (4th Cir. 1997), where a law enforcement officer had consent to search a residence for a fugitive. Id. at 1107. While looking for the fugitive in the basement, the officer observed some suspicious metal items on the floor. Id. He did not pause to examine those items at that time, but he instead proceeded to finish his sweep for the fugitive. Id. Once finished, he went back to take a closer look at the objects on the floor, this time recognizing them as drug paraphernalia. Id. More officers arrived and took a look at the paraphernalia, eventually using the presence of those items to obtain a search warrant for the house, which uncovered a gun and large quantities of drugs. Id. at 1108. That further search was held to have been constitutional under the plain-view doctrine. Id.

There are too many factual distinctions between Jackson and this case to permit Cravens' second look under the plain view doctrine. First, as government counsel

admitted at oral argument, there is no evidence in the record that Cravens looked at the same photos on November 27 that the officers viewed on November 20. Second, seven days elapsed between the first and second searches in this case, not a matter of minutes. Third, Cravens' "second look" led him to peruse more than just the child pornography images, so we cannot say that the November 27 search did not cause a further invasion of Loera's privacy. The plain view doctrine permits the warrantless seizure of evidence of criminal activity when police officers observe the evidence during a lawful search. United States v. Naugle, 997 F.2d 819, 822 (10th Cir. 1993). That doctrine cannot be used to justify Cravens' November 27 search.

The government also argues that Cravens' "second look" was justified under what it has termed the "foregone-conclusion exception" to the warrant requirement. This doctrine comes from several of our plain view cases where we have permitted the warrantless search of containers in plain view whose contents "are a foregone conclusion" because the container is "not closed," "transparent," or, if it is closed, "its 'distinctive configuration . . . proclaims its contents'" nonetheless. United States v. Corral, 970 F.2d 719, 725 (10th Cir. 1992). We have also held that the doctrine applies "where the police have already seen the contents of a seized container prior to conducting the search, [because] there is no significant additional invasion of privacy involved in searching the container." Id. at 725. We reject this argument for the same reasons as the government's plain view argument. Here, Cravens knew to a near certainty that the seized and re-searched CDs contained some child pornography, but he had no idea what else they contained. And, again, there is no evidence that

Cravens had previously seen the child pornography images that he viewed on November 27.

Thus, Cravens' November 27 search was unlawful because it exceeded the scope of the first warrant and none of the exceptions to the warrant requirement apply.

D. Reasonableness of the Searches Conducted Under the Second Warrant

Additionally, Loera argues that the child pornography evidence that Agent Nishida discovered when he executed the second warrant should have been suppressed because the second warrant was not supported by probable cause and no exceptions to the warrant requirement apply. We agree that the second warrant was not supported by probable cause and that the good faith exception is inapplicable here. However, the inevitable discovery doctrine supports the district court's denial of Loera's motion to suppress, and we affirm on that basis.

1. Second warrant was not supported by probable cause

We review whether a magistrate properly issued a search warrant by determining whether there was a "substantial basis" for probable cause in the affidavit submitted in support of the warrant. Illinois v. Gates, 462 U.S. 213, 236 (1983). Because we find that the November 27 search was unlawful, we must excise from the affidavit that Cravens filed in support of the second warrant all of the descriptions of child pornography that he unlawfully obtained during the second search and then determine whether "there was probable cause absent that information." United States v. Sims, 428 F.3d 945, 954 (10th Cir. 2005). The district court determined that the

second warrant remained supported by probable cause without the tainted descriptions. We disagree.

While "probable cause does not demand the certainty we associate with formal trials," Gates, 462 U.S. at 246, "[s]ufficient information must be presented to the magistrate to allow that official to determine probable cause; his action cannot be a mere ratification of the bare conclusions of others," id. at 239 (emphasis added). For example, "[a] sworn statement of an affiant that 'he has cause to suspect and does believe that' liquor illegally brought into the United States is located on certain premises" is not sufficient to support a finding that probable cause exists to search the premises. Id.

The child pornography descriptions that Agent Cravens obtained during the unlawful second search appear in paragraphs 24-27 of Cravens' affidavit. Once we excise those descriptions, all that remains substantively is Cravens statement that, "During the preview, the examiners identified four writable CDs which appeared to contain images of child pornography." ROA Vol. I at 120. This sentence does not support a finding of probable cause.

In United States v. Pavulak, the Third Circuit reviewed an affidavit to support a warrant to search for child pornography that contained language very similar to the bare-bones description left in the affidavit in our case, 700 F.3d 651, 661 (3d Cir. 2012). The warrant affidavit in Pavulak stated that an informant had seen the defendant "viewing child pornography" of females "between 16 and 18 years old," without providing any further details about what the images depicted. Id. at 657. The Third Circuit held that the affidavit lacked probable cause because it did not

allow the magistrate judge "to independently evaluate whether the contents of the alleged images [met] the legal definition of child pornography." Id. at 661. We find that analysis persuasive here. Agent Cravens' remaining statement that the CDs "appeared to contain images of child pornography" provides no detailed description of what the images depicted such that a magistrate could independently assess whether the images meet the legal definition of child pornography. ROA Vol. I at 120.

Therefore, the affidavit supporting the second warrant lacked probable cause absent the tainted information. We reverse the district court's contrary conclusion.

2. Good-faith exception inapplicable to these facts

Next, we consider whether the good faith exception to the exclusionary rule from United States v. Leon, 468 U.S. 897, 918 (1984), applies when police execute a search warrant that is based on information obtained through an unlawful predicate search. Disagreeing with the district court, we conclude that it does not. The Supreme Court's opinion in Leon and our opinion in United States v. Scales, 903 F.2d 765, 768 (10th Cir. 1990), dictate that the good faith exception does not apply in a case like the one before us because the illegality at issue stems from unlawful police conduct, rather than magistrate error, and therefore the deterrence purposes of the Fourth Amendment are best served by applying the exclusionary rule.

In United States v. Leon, the Supreme Court modified the exclusionary rule "so as not to bar the use in the prosecution's case in chief of evidence obtained by officers acting in reasonable reliance on a search warrant issued by a detached and

neutral magistrate but ultimately found to be unsupported by probable cause," 468 U.S. at 900. The Court reasoned that the purpose of the exclusionary rule is to deter police misconduct and in such a case "there is no police illegality and thus nothing to deter." Id. at 920. In this circuit, "Leon's good faith exception applies only narrowly, and ordinarily only when an officer relies, in an objectively reasonable manner, on a mistake made by someone other than the officer." United States v. Cos, 498 F.3d 1115, 1132 (10th Cir. 2007) (declining to apply good faith exception to warrantless search of apartment where officers mistakenly believed the person that consented to the search had the authority to do so); United States v. Herrera, 444 F.3d 1238, 1251 (10th Cir. 2006) (declining to apply good faith exception to state trooper who conducted a warrantless inspection of a truck based on the officer's mistaken belief the truck was a commercial vehicle subject to such inspection). Thus, Leon is inapplicable here where the mistake—the unconstitutional second search—was the fault of the officer, not the magistrate.

We considered whether Leon applied to a warrant affidavit based on tainted evidence in Scales, 903 F.2d at 768. There, we held that Leon did not apply to excuse a law enforcement officer's reliance on a search warrant where the facts in the warrant affidavit were obtained through an unlawful predicate seizure. In that case, DEA agents seized a suitcase that they believed contained drugs. Id. at 767. Then, they took the suitcase to a drug-sniffing canine team that signaled the suitcase did contain drugs. Id. Finally, after having had the suitcase in their possession for twenty-four hours, the agents applied for and obtained a warrant to search the

suitcase based on the probable cause provided by the canine alert. Id. Upon conducting the search, the agents discovered more than 2,000 grams of cocaine in the suitcase. Id. The defendant moved to suppress the cocaine evidence, arguing that the agents' initial seizure of the suitcase was unlawful because it was unsupported by probable cause. Id. at 767.

The district court in Scales denied the motion, finding that, even if the seizure of the suitcase was unlawful, the good faith exception ratified the agents' behavior. Id. We reversed, holding that Leon was inapplicable "[b]ecause the DEA agents were not acting in reliance on a search warrant when they seized the luggage and held it for more than twenty-four hours." Id. at 768. Our holding was informed by the reasoning in Leon that "Penalizing the officer for the magistrate's error, rather than his [or her] own, cannot logically contribute to the deterrence of Fourth Amendment violations." Id. at 768 (quoting Leon, 468 U.S. at 921) (alteration in original). Because the contraposition is also true—that penalizing an officer for his or her own error does contribute to deterrence—we determined that the exclusionary rule must apply to the agents' unlawful pre-warrant seizure of the suitcase. Id.

Scales and Leon control our outcome here. Cravens conducted an unlawful search of Loera's CDs on November 27 in the absence of a warrant. He included the tainted fruit that he uncovered during that search in the affidavit that he submitted in support of the second warrant. Cravens' warrant affidavit was facially valid, and therefore the magistrate did not error by issuing a warrant based upon it. Instead, the constitutional error came from Agent Cravens.

The government argues that Cravens acted in good faith because he "transparently informed the magistrate judge of the steps he had taken to obtain the descriptions he included in his affidavit." Aple. Br. at 40. Cravens' affidavit provided some information about the first search. It explained that, while executing the first search warrant, the FBI agents identified four CDs that contained child pornography and seized them. Then, Cravens wrote:

> On November 27, 2012, the writer, an FBI certified CART Technician, reviewed the four CDs, each of which are designated in attachment A, that were believed to contain child pornography. During the review of the CDs, the writer observed multiple pictures of children many of which are in various state of dress including the following images . . . .

ROA Vol. I at 50. However, that information was not sufficient to allow the magistrate to determine the constitutionality of the second search such that the magistrate can be said to have endorsed Cravens' pre-warrant conduct. Furthermore, even if it was, that would not affect our outcome. Tenth Circuit precedent dictates that the good faith exception does not apply at all when a warrant affidavit is based on tainted evidence from a prior, unlawful search.

Four other circuits have likewise concluded that Leon is inapplicable when an officer executes in good faith a search warrant that is based on unlawfully-obtained evidence. United States v. Scott, 731 F.3d 659, 664 (7th Cir. 2013) (holding that evidence discovered pursuant to a warrant based on illegally-obtained evidence will be inadmissible unless other, untainted information in the affidavit establishes probable cause); United States v. Mowatt, 513 F.3d 395, 405 (4th Cir. 2008) (holding that "Leon only prohibits penalizing officers for their good-faith reliance on

magistrates' probable cause determinations" and that the exclusionary rule operates to penalize officers for any unconstitutional conduct preceding a magistrate's involvement); United States v. McGough, 412 F.3d 1232 (11th Cir. 2005) (refusing to apply good faith exception where an unlawful entry into the defendant's apartment led to the officer's request for a search warrant); United States v. Vasey, 834 F.2d 782, 789 (9th Cir. 1987) (holding that good faith exception did not apply to a warrant that was based on information obtained in an illegal warrantless search because "[t]he constitutional error was made by the officer . . ., not by the magistrate"). At least two commentators support this analysis as well. See Wayne R. LaFave, Search & Seizure: A Treatise on the Fourth Amendment § 1.3(f) (5th ed. 2016) (explaining that, because courts rarely require affiants to prove that they obtained the evidence listed in an affidavit lawfully, "there is no reason why that process should, via Leon, shield that activity from full scrutiny at the suppression hearing"); Craig M. Bradley, The "Good Faith Exception" Cases: Reasonable Exercise in Futility, 60 Ind. L.J. 287, 302 (1985) (quoting Leon, 468 U.S. at 914) ("When the magistrate issued the warrant, he did not endorse past activity; he only authorized future activity. . . . [T]he function of the magistrate is to determine 'whether a particular affidavit establishes probable cause,' not whether the methods used to obtain the information in that affidavit were legal.").

However, five other circuits have concluded that the good faith exception can apply where an affidavit supporting a search warrant is tainted by illegally-obtained evidence in at least some limited circumstances. Three of those circuits apply the

good faith exception if the predicate search, although ultimately determined to be unlawful, was arguably lawful under the binding precedent in effect at the time of the search. United States v Bain, 874 F.3d 1, 22–23 (1st Cir. 2017) (applying good faith exception because binding precedent did not "clearly classify" as unlawful the conduct that invalidated the predicate search); United States v. Hopkins, 824 F.3d 726 (8th Cir. 2016) (applying good faith exception because the reasonableness of the illegal predicate search was "close enough to the line of validity" to make an officer's belief in the validity of the warrant objectively reasonable); United States v. Holley, 831 F.3d 322, 326–27 (5th Cir. 2016) (also applying "close enough to the line of validity" test). Two other circuits apply the good faith exception in these types of cases when (1) the predicate search was arguably reasonable and (2) the warrant affidavit truthfully conveyed the circumstances of the illegal predicate search to the magistrate judge. United States v. McClain, 444 F.3d 556, 566 (6th Cir. 2005) (applying Leon because the reasonableness of the predicate search was a close call and the warrant affidavit "fully disclosed" the circumstances surrounding the initial warrantless search); United States v. Thomas, 757 F.2d 1359 (2d Cir. 1985) (applying good faith exception because officer's affidavit fully described the unlawful, pre-warrant canine sniff that supplied probable cause for the warrant and there was "nothing more the officer could have or should have done" to be sure his search was legal). We cannot read Leon or Scales to support the rules adopted by these courts. When a magistrate issues a warrant based on illegally obtained evidence, typically the manner in which the affidavit evidence is obtained is not before the magistrate, and the

magistrate is not asked explicitly to endorse the evidence-gathering procedure. Even though some disclosure of the evidence-gathering technique may have occurred, that is not ordinarily the focus of an application for a warrant. Thus, we are unwilling to read a warrant as ratifying the information-gathering process of a search that preceded it. In any event, we are bound by Scales, which appears to us to have been correctly decided.

Therefore, the district court erred by finding that the good faith doctrine applied to the searches Agent Nishida conducted in execution of the second warrant.

3. Inevitable discovery doctrine supports denial of Loera's motion

Finally, we consider whether the government would have inevitably discovered the child pornography evidence on Loera's electronic devices. Loera argues that, because there was no probable cause to support the second warrant, all evidence discovered as a result of the execution of the second warrant should have been suppressed. The issue before us, then, is whether the FBI agents would have inevitably discovered the roughly 330 child pornography images on Loera's CDs and 730 child pornography images on Loera's laptop that Nishida found when he executed the second warrant. We conclude that they would have. Accordingly, we affirm the district court's denial of Loera's motion to suppress.

When evidence is obtained in violation of the Fourth Amendment, that evidence need not be suppressed if agents inevitably would have discovered it through lawful means independent from the unconstitutional search. United States v. Christy, 739 F.3d 534, 540 (10th Cir. 2014). The government is required to prove by a preponderance of the evidence that the unlawfully-obtained evidence would have been

discovered through lawful means. Id. The "lawful means" need not be a second, independent investigation. Id. Rather, the inevitable discovery doctrine will apply if there was "one line of investigation that would have led inevitably to the obtaining of a search warrant by independent lawful means but was halted prematurely by a search subsequently contended to be illegal." Id. (citations omitted). The key to applying this doctrine is to place the government officers in the "same positions they would have been in had the impermissible conduct not taken place," and, from that vantage point, to ask whether the government would have inevitably discovered the evidence lawfully. Nix v. Williams, 467 U.S. 431, 447 (1984).

Here, the district court's supportable findings demonstrate by a preponderance of the evidence that the FBI would have inevitably discovered the child pornography evidence on Loera's electronic devices through lawful means independent from Agent Cravens' unlawful second search. On November 26 (the day before the second search), the government lawfully had in its possession Loera's computers, external hard drives, iPhone, iPad, and thirteen CDs (nine without child pornography and four with child pornography).[4] The government had the authority under the first warrant to search Loera's electronic devices—most importantly his laptop and CDs—for evidence of computer fraud. The district court issued an explicit factual finding that, had the second warrant never been obtained, Agent Nishida would "have searched [Loera's

[4] As mentioned above, although Loera challenges the first search of these four CDs, he does not separately challenge their seizure were we to determine, as we have, that the first search was constitutional.

laptop] for evidence of electronic mail hijacking and computer fraud pursuant to the [f]irst [w]arrant." Dist. Ct. Op. at 24. The district court further found that, as part of that search, lawfully conducted pursuant to the parameters of the first warrant, Agent Nishida would have searched the electronic folders where he discovered child pornography when he executed the second warrant, including, the "My Documents" folder, the "Bookmarks" tab of Loera's internet browser, and a folder saved on the Desktop titled "Allmyfiles.txt." Id. at 24–25. The district court also accepted Nishida's statement that, had he found child pornography images on the laptop during a search conducted solely pursuant to the first warrant, he would have "alerted the case agent so that [he] could get a search warrant for child pornography." Id. at 25.

The laptop, including the specific files referenced above, contained over 730 images and 40 movies involving child pornography. Id. at 24. To take one specific example, the "Allmyfiles.txt" file, which the district court found Nishida would have lawfully opened pursuant to the first warrant, contained files called "Spycam 9yr Undress." Id. Such information would have been sufficient to establish probable cause to support a warrant to search all of the electronic devices belonging to Loera that the government had in its possession, including the four CDs that Agent Cravens searched unlawfully on November 27. That fact, combined with Agent Nishida's indication that he would have sought a warrant, allows us to conclude that the inevitable discovery doctrine applies in this case such that the evidence discovered pursuant to the second warrant did not need to be suppressed.

III. CONCLUSION

For the foregoing reasons, we AFFIRM the orders of the district court denying the defendant's motion to suppress and motion for reconsideration.