PRECEDENTIAL

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

_____

Nos. 09-3500 and 09-3501

_____

UNITED STATES OF AMERICA

v.

SALVATORE STABILE

Appellant

_____

On Appeal from the United States District Court
for the District of New Jersey
(Criminal Nos. 08-cr-00145 & 09-cr-00241-001)
District Judge: Honorable Stanley R. Chesler

_____

Argued on December 16, 2010

Before: JORDAN, HARDIMAN and VAN ANTWERPEN,
Circuit Judges.

(Filed February 1, 2011)

Robert W. Ray, Esq. [**ARGUED**]
Ross M. Bagley, Esq.
Pryor Cashman LLP

7 Times Square
New York, NY 10036-6569
Counsel for Appellant

Paul J. Fishman
George S. Leone
John F. Romano [**ARGUED**]
Office of United States Attorney
970 Broad Street, Suite 700
Newark, NJ 07102-2535
Counsel for Appellee

OPINION OF THE COURT

VAN ANTWERPEN, *Circuit Judge*.

Defendant-Appellant Salvatore Stabile ("Stabile") pleaded guilty to one count of bank fraud in violation of 18 U.S.C. § 1344, waived a jury trial and stipulated to facts for a bench trial with regard to three counts of receipt of child pornography and one count of possession of child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B). The District Court found Stabile guilty of these child pornography charges. Stabile retained the right to appeal the District Court's ruling on his suppression motions. All charges were consolidated for sentencing, and the District Court sentenced Stabile to concurrent sentences of 78 months' imprisonment on each count. Stabile appeals the District Court's denial of his motion to suppress as well as the sentence the District Court imposed.

The facts in this case are complex and they relate to a number of issues. In particular we face issues regarding the scope of the plain view doctrine in the context of computer searches. We will affirm the District Court's suppression order. Stabile also appeals his sentence, however we decline to exercise our jurisdiction over the sentencing appeal because Stabile waived his right to appeal his sentence.

I. Facts

A. Background

Prior to the beginning of the investigation, Stabile resided in Mahwah, New Jersey, with Debbie Deetz. Deetz believed that she was married to Stabile. However, Stabile was already married and had not divorced his first wife. *Appx*. at A-453. The house shared by Stabile and Deetz was secured by a mortgage and home equity credit line in the name of Stabile's brother. Stabile defaulted on these loans and tried to mask his default by passing more than $156,000 in counterfeit checks. These counterfeit checks initially formed the basis for investigating Stabile.

B. Search of Stabile's House

At 1:00 p.m. on July 24, 2006, Secret Service Special Agents Christopher Albanese and John Croes, and Detective Joseph Nieciecki of the Bergen County Sheriff's Department, arrived at Stabile's house to question Stabile about counterfeiting checks. Stabile was not at home, but Deetz answered the door, invited the agents inside, asked the officers to sit at a table near the living room, and offered them something to drink. The officers informed Deetz of the

purpose of their visit and explained that they suspected that Stabile had engaged in financial crimes. Albanese then asked Deetz for consent to search the house. Albanese provided Deetz with a consent form and informed Deetz that she could refuse consent. Deetz reviewed the consent form for approximately thirty minutes and then signed it. Deetz testified that one of the reasons she voluntarily signed the form was so she herself could find out about Stabile's deceptive financial practices.

Deetz granted consent orally and in writing by signing a consent form.[1] Without a search warrant but with Deetz's

[1] The "Consent To Search" form states, in its entirety:

> "I, Debbie Deetz, have been informed of my constitutional right not to have a search made of the premises and/or automobile mentioned without a search warrant. I have also been informed of my right to refuse to consent to such a search. However, I hereby authorize Christopher Albanese and John Croes, Special Agents, United States Secret Service to conduct a complete search of the premises and/or automobile at 181 Miller Road, Mahwah, NJ. These (officers or agents) are authorized by me to take from the premises and/or automobile any letters, papers, materials or other property which is contraband or evidence in the nature of financial crimes. I understand that this contraband or evidence may be used against me in a court of law. This written permission is being given by me to the above named persons

consent, the agents began a search of the house. During the course of the search, Deetz led the agents around the house, provided the agents with documents related to Stabile's finances, and showed the agents the locations of several computers. Next to one computer, the agents found check stock, check writing software, photocopies of checks, copies of previously-passed fraudulent checks, two printers, and checks with an alias. Deetz also showed the agents two computers and several hard drives in the basement of the house. At the suppression hearing, Deetz testified:

> Q. And who pointed out those hard drives to the law enforcement officers?
> A. I [Deetz] did.
> Q. Did you provide consent for the officers to search those computers?
> A. Yes, I did.

Appx. at A-467. The agents then called the Bergen County Prosecutor's Office, which sent two members from its Computer Crimes Unit to disconnect the hard drives. Deetz showed the recently-arrived Bergen County officers the locations of the computers and the hard drives. Deetz watched the officers remove the hard drives. When one officer had difficulty removing a hard drive, Deetz asked the officer if he needed a screwdriver. The officer replied that he

---

> voluntarily and without threats, duress, or promises of any kind. I understand that I may ask for and receive a receipt of all things taken."

The form was then signed by Albanese, Croes, and Deetz. *Appx*. at A-195.

did, so Deetz got a screwdriver from Stabile's toolbox and gave it to the officer. At approximately 6:00 p.m., the Bergen County officers Justified the house, taking with them six hard drives. Stabile was not present in his house at any point during this search. In fact, the search had been completed when Stabile arrived home, at approximately 7:15 p.m.

During their search of Stabile's house, the agents also found several DVDs in a desk bearing labels which led the agents to believe the DVDs contained child pornography.[2] The officers seized the DVDs but, upon a later viewing of their contents, determined that they did not contain child pornography.

When Stabile arrived home, Deetz waited outside the house while the agents interviewed Stabile. Although the agents attempted to question Stabile, Stabile refused to answer questions without an attorney present. When informed that Deetz had already consented to the search, Stabile attempted to revoke Deetz's consent by stating "I take it back." The agents then departed. It is undisputed that Stabile did not request the return of his property at this time. In fact, Stabile did not request return of his seized property until February 15, 2008, when he filed a motion to return property.

---

[2] One such DVD was labeled "Japanese Mature Women VS. Ripe Boy Movies." Agent Albanese also opined in his affidavit attached to the warrant application that the "images of males depicted on the labels are . . . images of minors." *Appx*. at A-127-28.

C. Issuance of the State Search Warrant

Although the agents obtained the six hard drives on July 24, 2006, Agent Albanese did not apply for a state search warrant until October 19, 2006 because he was assigned to a Secret Service security detail for the President and other high officials. Finally, Albanese applied for a state search warrant on October 19, 2006 in New Jersey Superior Court in Morris County.[3] The state search warrant was issued and authorized search of the computer hard drives[4] for evidence of "both financial crimes and the possession of child pornography." Probable cause to search the hard drives for evidence of financial crimes was based on the check stock, printed checks, and check printing software found in Stabile's house.

---

[3] Stabile's home was in Bergen County, New Jersey, but the investigation was centered in Morris County, New Jersey, where Stabile allegedly delivered three counterfeit checks to an attorney.

[4] The Morris County Inventory Receipt identified six hard drives:

> (1) Western Digital 40 GB 3.5 inch HDD, Ser # WMAAT1253959
> (1) Western Digital 120 GB 3.5 inch HDD, Ser # WMAAT2323593
> (1) Western Digital 2559.8 MB 3.5 inch HDD, Ser # WM3491805359
> (1) Seagate 3.5 inch HDD, Ser # LAA62086
> (1) Quantum 3.5 inch HDD, Ser # 824909331341
> (1) Samsung 6.8 GB 3.5 inch HDD, Ser # 0149J1FKB07213

Probable cause to search for evidence of child pornography was based on the DVDs found in a desk in Stabile's house. The affidavit submitted by Albanese stated that "This Affiant believes these DVDs contain labels with language that refers to mature women and young boys and contains images of minors." Unbeknownst to Albanese, between the July 24, 2006 seizure of the DVDs and the October 19, 2006 state search warrant application, state law enforcement officers had already viewed the DVDs and determined that they did *not* contain child pornography. Albanese was not aware that the DVDs had been viewed and determined not to contain child pornography when he applied for the state search warrant on October 19, 2006. Accordingly, the state search warrant obtained on October 19, 2006 stated that it authorized search of the hard drives for evidence of *both* financial crimes and child pornography.

On November 16, 2006, after the issuance of the state search warrant, Agent Albanese traveled to the Bergen County Prosecutor's Office where the evidence was stored. Albanese picked up the evidence and transported it to the Morris County Prosecutor's Office. During this process, but *before* Albanese brought the hard drives to the Morris County Prosecutor's Office, Albanese learned that the DVDs from the desk had been viewed and were found not to contain child pornography. *Appx*. at A-726. Upon arrival, Albanese "informed everybody," including the detective who would perform the forensic search, that there was a "problem" with the state search warrant as it related to child pornography. *Appx*. at A-726.

D. Execution of State Search Warrant

In mid-November, 2006, Detective Vanadia, a forensic specialist at the Computer Crimes Unit of the Morris County Prosecutor's Office, received the hard drives. Vanadia had been instructed to search *only* for evidence of financial crimes and told that if he came across child pornography, he was to stop his review and contact the Secret Service. *Appx*. at A-528, A-562, A-580-81, A-727-28.

With these instructions, Detective Vanadia commenced his forensic hard drive search. He began with the 120 GB hard drive (Western Digital 120 GB 3.5 inch HDD, Ser # WMAAT2323593). During this search, Vanadia noted numerous suspicious folders. One such folder was entitled "Kazvid." Vanadia understood this folder to reference "Kazaa," a peer-to-peer file sharing program used to share music, movies, pictures, and programs. *Appx*. at A-532. Vanadia also testified that, in his experience, Kazaa has been used to share and distribute child pornography.

Detective Vanadia then "highlighted" the Kazvid folder, a procedure that allowed him to view a list of file names contained in the folder. Vanadia later testified that he highlighted the Kazvid folder not because it necessarily contained child pornography but because – as a suspicious folder – it could harbor evidence of any sort of crime, including a financial crime. *Appx*. at A-536-37, A-581-82. Vanadia also testified that, in his experience, people hoping to conceal the contents of a folder or file would often mislabel or otherwise disguise those folders or files. *Appx*. at A-537, A-582. However, Vanadia did acknowledge that when he viewed the file names in the "Kazvid" folder, the thought that it may contain child pornography did cross his mind. *Appx*. at A-588.

After highlighting the "Kazvid" folder, Detective Vanadia observed a list of file names with file extensions indicating video files and file names suggestive of child pornography.[5] At this point, although Vanadia admitted that he suspected child pornography and did not believe these video files contained evidence of financial crimes, Vanadia proceeded to open twelve different video files within the Kazvid folder. *Appx*. at A-534-35, A-591-92. Vanadia testified that he opened these twelve files to "confirm" that they contained child pornography rather than something else (such as adult pornography). *Appx*. at A-534-35, A-591-92. After "confirming" that these files did contain child pornography, Vanadia contacted the prosecutor, who instructed Vanadia to cease his review of the hard drive. Agent Albanese was notified of Vanadia's findings.

E. The Federal Search Warrants

After learning of Detective Vanadia's discovery of child pornography, Agent Albanese applied for a federal search warrant on April 23, 2007, which was issued on April 24, 2007. This was the first federal search warrant issued in this case. The affidavit for the first federal search warrant was based on probable cause gleaned from the *names* of the files in the Kazvid folder, not the contents of the files

[5] These files had names such as "PTHC" (pre-teen hardcore), "PEDO" (pedophile-related), "6YO" (six-year-old), and "8YO" (eight-year-old). Some file names identified a sex act and the gender of the participant following the "YO" age designation.

themselves.[6] At no point in the first federal search warrant application did the affidavit state that Vanadia had opened the files in the Kazvid folder.

On April 24, 2007, based on the file names found in the Kazvid folder on the 120 GB drive, a magistrate issued the first federal search warrant authorizing further investigation. However, by mistake the first federal search warrant only authorized the search of a *different* hard drive owned by Stabile, the 40 GB hard drive (Western Digital 40 GB 3.5 inch HDD, Ser # WMAAT1253959), rather than the 120 GB hard drive Detective Vanadia had examined.

Around April 25, 2007, Agent Joseph Tokash executed the first federal search warrant and searched the 40 GB hard

---

[6] The affidavit stated:

> 26. While running a search for the counterfeit check numbers, Detective Vanadia began reviewing the file folders on the DRIVE to locate a commercially available check processing program which, based upon his training and expertise, he knew was commonly used in the production of counterfeit checks. While conducting this review, Detective Vanadia observed a file folder labeled "Kazaa Vid" that contained approximately 410 saved files. Detective Vanadia further observed that several of these files contained titles with the abbreviation "PTHC" as well as file names including "6yopedo" and "9yofuck."

Appx. at A-164.

drive. This search resulted in the discovery of two videos and 86 thumbnail images of child pornography. *Appx.* at A-189.

Based on the discovery of child pornography on the 40 GB hard drive, Agent Albanese sought a second federal search warrant on September 20, 2007 to search the other five hard drives (including the 120 GB hard drive originally searched by Detective Vanadia in November, 2006 pursuant to the state search warrant for financial information). The second federal search warrant was issued authorizing the search of the remaining five hard drives (excluding the previously-searched 40 GB hard drive). Agent Tokash executed the second federal search warrant and discovered more than 200 videos and 100 thumbnail images depicting child pornography.

F. Arrest and Prosecution

On October 10, 2007, Stabile was arrested and charged with receipt of child pornography in violation of 18 U.S.C. § 2252A(a)(2)(B) and indicted on February 21, 2008. On February 2, 2009, a superseding indictment was filed charging Stabile with three counts of receipt of child pornography in violation of 18 U.S.C. § 2252A(a)(2)(B) and one count of possession of child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B). In a separate prosecution, on May 9, 2008, Stabile was charged with bank fraud under 18 U.S.C. § 1344.

G. Stabile's Motion to Suppress and the District Court's Decision

On July 1, 2008, Stabile moved to suppress evidence seized from his house on July 24, 2006, arguing (1) that the Government's warrantless seizure of the hard drives for three months without a search warrant was unreasonable, and (2) that pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978), the state search warrant authorizing search for child pornography was invalid because the DVDs from the desk which formed the alleged "probable cause" did not actually contain child pornography.

In September, 2008, the District Court held a two-day evidentiary hearing. On November 3, 2008, the parties submitted post-hearing briefs. Stabile argued that: (1) Detective Vanadia's search exceeded the scope of the search for financial information authorized by Deetz's consent and the state search warrant; (2) Stabile withdrew Deetz's consent when he got home and therefore, pursuant to *Georgia v. Randolph*, 547 U.S. 103 (2006), the Government waited an unreasonable period of time to secure the state search warrant; and (3) suppression of evidence was required as a result of this unreasonable search. On December 4, 2008, the District Court again heard oral argument.

On January 21, 2009, the District Court denied Stabile's motion to suppress. *United States v. Stabile*, Crim. No. 08-145 (SRC), 2009 U.S. Dist. LEXIS 4263 (D.N.J. Jan. 21, 2009). The District Court concluded that the search of Stabile's house was a valid consent search, that Stabile could not "revoke" Deetz's prior consent under *Georgia v. Randolph*, that the Government's delay in obtaining a state search warrant was not unreasonably long, and that, under the inevitable discovery doctrine, the evidence obtained from the search of the 120 GB hard drive need not be suppressed.

On February 3, 2009, Stabile filed a motion for reconsideration in which he argued that, *inter alia*, the District Court committed legal error by applying the inevitable discovery doctrine rather than the independent source doctrine, and that this error required correction. On March 13, 2009, the District Court denied the motion for reconsideration, reaffirming its application of the inevitable discovery doctrine and holding that the evidence would also be admissible under the independent source doctrine. *United States v. Stabile*, Crim. No. 08-145 (SRC), 2009 U.S. Dist. LEXIS 20275 (D.N.J. Mar. 13, 2009).

H. Stipulated Facts Trial and Guilty Verdict (Child Pornography Counts)

Following denial of his motion to reconsider, Stabile executed stipulations with the Government, including an admission that he knowingly received and possessed child pornography. Stabile also executed a stipulation preserving his right to appeal the denial of the motion to suppress. The parties also stipulated that the applicable Guidelines offense level was 26. Finally, Stabile stipulated that he "voluntarily waives the right to file any appeal . . . including but not limited to an appeal under 18 U.S.C. § 3742 . . . which challenges the sentence imposed by the sentencing court in this case if that sentence falls within or below the Guidelines range that results from the agreed total Guidelines offense level of 26."

On April 3, 2009, Stabile was advised in court about the impact of the stipulations, including the appellate waiver. Stabile knowingly and voluntarily agreed to the stipulations.

After a bench trial, the District Court found Stabile guilty of all four counts in the Superseding Indictment pertaining to child pornography.

I. Guilty Plea (Bank Fraud Count)

On April 3, 2009, Stabile was charged in a one-count information with bank fraud in violation of 18 U.S.C. § 1344, executed a written Plea Agreement, and entered a guilty plea to the information.

J. Consolidated Sentencing Proceeding

All of Stabile's convictions were consolidated for sentencing. A sentencing hearing was held on August 12, 2009. The District Court calculated the applicable Guidelines range using offense level 26 – the level to which Stabile had agreed. Stabile's criminal history category was level III. The District Court determined that Stabile's Guidelines range was 78 to 97 months. The District Court also heard arguments from Stabile that the child pornography guideline, specifically U.S.S.G. § 2G2.2, should be afforded little deference. After considering these arguments and the 18 U.S.C. § 3553(a) factors, the District Court imposed concurrent 78-month sentences on each count.

K. Appeal

On August 21, 2009, Stabile filed an appeal challenging the District Court's denial of his motion to suppress and his sentence.

II. Jurisdiction

The District Court had jurisdiction under 18 U.S.C. § 3231. We have jurisdiction over Stabile's appeal of the District Court's denial of his motion to suppress under 28 U.S.C. § 1291 and over his challenge to his sentence under 18 U.S.C. § 3742(a).

III. Issues and Analysis

On appeal, Stabile challenges the District Court's denial of his motion to suppress as well as the sentence the District Court imposed.

III.A. Motion to Suppress

Stabile first appeals the District Court's denial of his motion to suppress evidence of child pornography obtained from Stabile's six computer hard drives. Stabile alleges myriad violations of his Fourth Amendment rights and concludes that the fruits of these allegedly illegal searches must be suppressed. We consider Stabile's arguments in chronological order of the investigation: (1) search of Stabile's house; (2) seizure of Stabile's six computer hard drives; (3) delay in obtaining the state search warrant; and (4) search of the hard drives. Finding no Fourth Amendment violations requiring suppression, we will affirm.

We review the District Court's denial of a motion to suppress for clear error as to the underlying factual determinations but exercise plenary review over the District Court's application of law to those facts. *See United States v. Bond*, 581 F.3d 128, 133 (3d Cir. 2009); *United States v. Perez*, 280 F.3d 318, 336 (3d Cir. 2002).

III.A.1. Search of Stabile's House

Stabile first argues that the Government's July 24, 2006 warrantless search of his house violated the Fourth Amendment. This argument fails because Deetz consented to the search.

The Fourth Amendment prohibits unreasonable searches and seizures. *See Illinois v. Rodriguez*, 497 U.S. 177, 183 (1990); *United States v. Price*, 558 F.3d 270, 277 (3d Cir. 2009); *Payton v. New York*, 445 U.S. 573, 586 (1980). In general, a "warrantless entry into a person's house is unreasonable *per se*." *See Payton*, 445 U.S. at 586. However, there are exceptions to this rule. *See Jones v. United States*, 357 U.S. 493, 499 (1958).

Consent is an exception to the "requirements of both a warrant and probable cause." *Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973); *see Florida v. Jimeno*, 500 U.S. 248, 250-51 (1991) (approving consent searches because a search permitted by consent is reasonable). Consent must be given voluntarily, *Bumper v. North Carolina*, 391 U.S. 543, 548 (1968), and voluntariness may be gleaned from considering a range of factors. *See Price*, 558 F.3d at 279; *United States v. Kim*, 27 F.3d 947, 955 (3d Cir. 1994). The individual giving consent must also possess the authority to do so, *see Rodriguez*, 497 U.S. at 181, and "the consent of one who possesses common authority over premises or effects is valid as against the absent, nonconsenting person with whom that authority is shared," *United States v. Matlock*, 415 U.S. 164, 170 (1974). Common authority rests not on property rights but "rather on mutual use of the property by persons generally having joint access or control . . . so that it is reasonable to

recognize that any of the cohabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit the common area to be searched." *Id*. at 172 n.7. Finally, "a warrantless search of a shared dwelling for evidence over the express refusal of consent by a physically present resident cannot be justified as reasonable as to him on the basis of consent given to the police by another resident." *Georgia v. Randolph*, 547 U.S. 103, 120 (2006).

Here, Deetz had authority to consent and voluntarily consented. Deetz had common authority to consent to a search of the house because, as a cohabitant, she mutually used the property along with Stabile and exercised joint access and control over the house. *See Matlock*, 415 U.S. at 172 n.7. Deetz's mistaken belief that she was married to Stabile does not alter the analysis because an unmarried cohabitant has authority to consent to a search of shared premises. *See id*. at 176. Finally, we note that at the time Deetz granted consent, Stabile was not present. Stabile's absence distinguishes this case from *Georgia v. Randolph*, which applies only when a "physically present resident" refuses consent. 547 U.S. at 120. Therefore, because Deetz exercised her access and control over the premises absent any contemporaneous refusal by a co-resident, she had authority to consent at the time of the search.

We also conclude that Deetz's consent was voluntary. "[W]e determine the voluntariness of a consent by examining the totality of the circumstances." *Price*, 558 F.3d at 278; *Schneckloth*, 412 U.S. at 227. We consider such factors as "age, education, and intelligence of the subject; whether the subject was advised of his or her constitutional rights; the

length of the encounter, the repetition or duration of the questioning; and the use of physical punishment." *Price*, 558 F.3d at 278; *see Schneckloth*, 412 U.S. at 226. The "'setting in which the consent was obtained [and] the parties' verbal and non-verbal actions'" are also relevant. *Price*, 558 F.3d at 278 (quoting *United States v. Givan*, 320 F.3d 452, 459 (3d Cir. 2003)). Finally, even though Deetz was told she could refuse, the Government need not inform the subject of his right to refuse consent. *Schneckloth*, 412 U.S. at 227 (not essential for prosecution to show that the consenter knew of the right to refuse consent in order to establish that the consent was voluntary); *Kim*, 27 F.3d at 955.

Here, Deetz, an educated person, invited the officers into her house. She asked the officers to sit and offered them drinks. The officers asked Deetz to sign a written consent form, and Deetz thought about whether to sign it for thirty minutes before she did, in fact, sign it. Deetz also orally consented to the search. After signing the form, Deetz assisted the officers in their search of the house by leading them to several computers and, later, providing one officer with a screwdriver to help remove a hard drive. Considering the totality of the circumstances, there is no indication that Deetz's consent was involuntary.

Therefore, because Deetz had the authority to consent to a search of the house and because Deetz voluntarily consented to the search, the initial warrantless search of the house did not violate the Fourth Amendment.

III.A.2. Seizure of Stabile's Six Hard Drives

Although Stabile concedes in his brief that the warrantless seizure of the six computer hard drives is controlled by the case law[7] of this circuit, he nevertheless contests the seizure and makes two arguments in his brief. First, Stabile contends that the Government lacked authority to seize the six hard drives because Deetz could not consent to a seizure of the drives. Second, Stabile argues that even if Deetz *did* validly consent to the seizure of the hard drives, the Government's seizure was still unreasonably overbroad. Both of these arguments lack merit.

III.A.2.a. Consent to Seize Hard Drives

We first consider whether Deetz consented to the seizure of the hard drives. This analysis parallels the analysis of whether Deetz could consent to the search of the house: Deetz must have had authority to consent to the seizure of the hard drives, and she must have consented voluntarily.

We believe Deetz had authority to consent to the seizure of the six hard drives. The "authority to consent" determination is complicated because computers often contain segregated blocks of information. We begin with the same proposition that authority to consent derives from "mutual use of the property by persons generally having joint access or control for most purposes." *Matlock*, 415 U.S. at 171 n.7; *see Frazier v. Cupp*, 394 U.S. 731, 740 (1969) (joint use of duffel bag gave third party authority to consent to search of bag). However, a third party lacks authority to consent to a search of an area in which the target of the search

[7] Stabile cites *United States v. King*, 604 F.3d 125 (3d Cir. 2010).

has not "relinquished his privacy." *United States v. King*, 604 F.3d 125, 137 (3d Cir. 2010); *see United States v. Block*, 590 F.2d 535 (4th Cir. 1978) (holding that mother had authority to consent to search of son's bedroom but not to son's locked footlocker kept under his bed); *Randolph*, 547 U.S. at 135 (Roberts, C.J., dissenting) ("To the extent a person wants to ensure that his possessions will be subject to a consent search only due to his *own* consent, he is free to place these items in an area over which others do *not* share access and control, be it in a private room or a locked suitcase under a bed."). Thus if a person has not "relinquished his privacy" in some files on a computer or in a subset of information contained on the computer, a third party would have no authority to consent to the search or seizure of those segregated materials.

Additionally, multiple people may use the same computer and store information on the same hard drive. It is more difficult to determine whether joint access and control exists over information stored on a computer than the contents of a duffel bag. *See Frazier*, 394 U.S. at 740. Indeed, attempting to make these determinations would force courts to engage in the very "metaphysical subtleties" the Supreme Court expressly rejected in *Frazier* when the defendant unsuccessfully argued that a third party had "actual consent" only to use one compartment of a duffel bag. *Id*. Thus we are faced at the outset with a conceptual question: is a computer more like a shared duffel bag, *see Frazier*, 394 U.S. 731, or more like a locked footlocker under the bed? *See Block*, 590 F.2d 535. We believe the answer depends on factors such as the identity of the user(s), whether password protection is used, and the location of the computer in the house. *See United States v. Andrus*, 483 F.3d 711,718-20

(10th Cir. 2007) (listing factors to consider when evaluating validity of third party consent to search computer).

Recently, in *United States v. King*, where the defendant "placed his hard drive inside the computer" owned by another person but which the two of them shared, and did not use password protection, the defendant "assumed the risk" that the other person would "consent to its seizure." 604 F.3d at 137. Conversely, in *Trulock v. Freeh*, the defendant utilized password protection to protect his private computer files, and, therefore, the Fourth Circuit determined that the defendant had *not* assumed the risk that his co-user "would permit others to search his files." 275 F.3d 391, 403 (4th Cir. 2001). Moreover, in *King*, we considered whether the holding of *Georgia v. Randolph* that a "present and objecting resident can override another resident's consent to search a home" applied to the seizure of a computer. 604 F.3d at 130. The *King* court determined that *Randolph* was meant to apply only to dwellings and, therefore, that a "present and objecting resident" could *not* override another resident's consent to seize a shared computer which contained a personal hard drive but lacked user-specific password protection. *Id.* at 137; *see Andrus*, 483 F.3d at 721 (objectively reasonable to perceive third party consent where consenter was a "user" of the computer).

Here, the facts weigh in favor of a determination that Deetz had the authority to consent to a search and seizure of the shared hard drives. First, the computer was not password-protected. The failure to use password protection indicates that Stabile relinquished his privacy in the contents of the computer. *Cf. Trulock*, 275 F.3d at 403 (third party did not have authority to consent to search of joint computer user's

password-protected files). In distinction to *King*, here Stabile was not present and objecting to the search of the computer. Moreover, all of the computers and seized hard drives were located in common areas of the home, such as on the main floor and in the basement, rather than in a private bedroom. *See Andrus*, 483 F.3d at 719 (third party authority to consent generally upheld when computer located in common area accessible to family members). These factors indicate that, under the totality of the circumstances, Deetz had unfettered access to the hard drives and had authority to consent to the seizure of all of them.

Deetz's consent to the seizure of the six hard drives was voluntary. As previously discussed, Deetz signed the consent form and told the investigator to "go ahead and take them [the hard drives]." Moreover, Deetz's consent may also be inferred from the assistance she provided to the officers. Specifically, when one officer had difficulty extracting a hard drive from the computer terminal, Deetz obtained a screwdriver from Stabile's toolbox and gave it to the officer. *See United States v. Al-Marri*, 230 F. Supp. 2d 535, 539 (S.D.N.Y. 2002) (defendant objectively consented to search of his computer by, *inter alia*, assisting the investigation by helping FBI agents pack his computer in a carrying case).

Thus we conclude that Deetz had authority to consent to the seizure of the six hard drives and did so voluntarily.

III.A.2.b. Scope of Seizure of Hard Drives

Pursuant to Deetz's consent, the officers searched the house and seized six computer hard drives. Stabile argues that even assuming Deetz validly consented to this search and

seizure, the seizure of six *entire* hard drives was unreasonable because it was unconstitutionally overbroad. Stabile notes that by seizing six entire hard drives, the Government also seized personal emails and other information not related to financial crimes. Therefore, according to Stabile, the Government's failure to "segregate" data on-site (at Stabile's house) renders this seizure unconstitutionally overbroad. The Government defends the seizure on the grounds that Deetz did not limit the scope of her consent, that evidence of financial crimes could be found anywhere on any computer hard drive, and that the practical considerations of investigating and seizing electronic evidence counsel against on-site data collection. We agree with the Government and reject Stabile's argument.

The seizure of the six entire hard drives was reasonable. First, except for the restriction as to financial crimes, Deetz did not limit the scope of her consent in any way. *See Jimeno*, 500 U.S. at 251-52 (requiring explicit limitation on consent). Second, a broad seizure was required because evidence of financial crimes could have been found in any location on any of the six hard drives, and this evidence very likely would have been disguised or concealed somewhere on the hard drive. *See United States v. Adjani*, 452 F.3d 1140, 1150 (9th Cir. 2006). Third, as a practical matter, "[w]hen a search requires review of a large collection of items, such as papers, 'it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized.'" *United States v. Williams*, 592 F.3d 511, 519-20 (4th Cir. 2010) (quoting *Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976)). Finally, Stabile argues for an "on-site" search requirement, but the practical realities of

computer investigations preclude on-site searches. For example, a hard drive search requires a "controlled environment." *United States v. Hay*, 231 F.3d 630, 637 (9th Cir. 2000). Computer searches are also time consuming and require trained forensic investigators. *See United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999). In short, such on-site searches would be "fraught with difficulty and risk," *United States v. Hill*, 459 F.3d 966, 974 (9th Cir. 2006), and cannot be rushed by a cursory on-site search.[8] All these reasons suggest that the seizure of the six entire hard drives was reasonable.

Lastly, although Stabile attempted to revoke Deetz's consent when he returned home later on the day of the search

[8] Stabile heavily relies on *United States v. Tamura*, 694 F.2d 591 (9th Cir. 1982). His reliance is faulty. *Tamura*, a case dealing with the overbroad seizure of *paper* records, "preceded the dawn of the information age." *Comprehensive Drug Testing*, 621 F.3d 1162, 1169 (9th Cir. 2010) (discussing *Tamura*). And even the Ninth Circuit recognized that *Tamura* needed to be "updated . . . to apply to the daunting realities of electronic searches." *Id*. at 1177. Thus while the concerns of *Tamura* may remain valid, we hesitate to apply the procedures *Tamura* outlined for proper searches of physical evidence to the procedures required to searches of electronic evidence. *See generally*, *id*., at 1175-78. Finally, we note that although the *Tamura* court found the overbroad seizure of documents "unreasonable," the court concluded that suppression was not required. *Tamura*, 694 F.2d at 696-97. Thus, even if *Tamura* were to apply, it would not require suppression here either.

by stating "I take it [Deetz's consent] back" to the investigating agents, this revocation is ineffective. Stabile could not revoke Deetz's consent to search the house because Stabile was not "physically present" at the time Deetz consented. *Randolph*, 547 U.S. at 120. Nor can Stabile revoke Deetz's consent to the seizure of the shared hard drives because Stabile had "relinquished his privacy" in the hard drives, *King*, 604 F.3d at 137, and thus "assumed the risk" that a third party could consent to their search or seizure, *Matlock*, 415 U.S. at 171.

III.A.3. Delay in Obtaining the State Search Warrant

Stabile also argues that the Government unreasonably delayed by waiting almost three months[9] before obtaining the state search warrant and searching the seized hard drives. This argument raises some difficult issues.

Initially, we note that Stabile's reliance on *United States v. Mitchell*, 565 F.3d 1347 (11th Cir. 2009), and *United States v. Dass*, 849 F.2d 414 (9th Cir. 1988), is misplaced. *Mitchell* and *Dass* held, respectively, that a 21-day delay and a 7- to 23-day delay between seizure and search were unreasonable when the warrantless seizures were based on *probable cause*, not consent. *Mitchell*, 565 F.3d at 1349-51; *Dass*, 849 F.2d at 414-15. This distinction matters. The *Mitchell* court carefully policed the temporal delay in obtaining a search warrant because each passing day "infringes possessory interests protected by the Fourth

[9] The officers seized the hard drives on July 24, 2006, but the state search warrant was not issued until October 19, 2006.

Amendment's prohibition on 'unreasonable searches.'" *Mitchell*, 565 F.3d at 1350 (quoting *United States v. Jacobsen*, 466 U.S. 109, 124 (1984)). But where a person *consents* to search and seizure, no possessory interest has been infringed because valid consent, by definition, requires *voluntary* tender of property.[10]

Of course, "a seizure lawful at its inception can nevertheless violate the Fourth Amendment if its manner of execution unreasonably infringes possessory interests protected by the Fourth Amendment's prohibition on 'unreasonable seizures.'" *Jacobsen*, 466 U.S. at 125. To determine whether the seizure became unreasonable, this Court "must balance the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion." *United States v. Place*, 462 U.S. 696, 703 (1983); *see United States v. Martin*, 157 F.3d 46, 54 (2d Cir. 1998) ("even a seizure based on probable cause is unconstitutional if police act with unreasonable delay in securing a warrant").

Here, we balance the interests at stake to determine whether the three month delay was reasonable. Stabile relies on *Mitchell*'s focus on the property interest at stake in one's computer:

> Computers are relied upon heavily for personal and business use. Individuals may store personal letters, e-mails, financial information,

[10] As noted, there was no request for return of the hard drives until February 15, 2008, which was well after the state search warrant had been obtained.

> passwords, family photos, and countless other items of a personal nature in electronic form on their computer hard drives. . . . If anything, this consideration applies with even greater force to the hard drive of a computer, which is the digital equivalent of its owner's home, capable of holding a universe of private information.

Mitchell, 565 F.3d at 1351-52. Stabile also argues that "his job required him to have constant access to a computer." *Appx*. at A-202; Appellant's Br. 23.

Stabile's actions undermine his argument. First, it is undisputed that Stabile did not ask for the return of his hard drives until February 15, 2008 – *eighteen months* after the initial seizure of the hard drives.[11] *See United States v. Johns*, 469 U.S. 478, 487 (1985) (defendants who "never sought return of the property" cannot argue that delay adversely affected Fourth Amendment rights). And when asked why he never requested the return of the hard drives, Stabile testified, "I just assumed that perhaps that they didn't find anything and it was going to go away." *Appx*. at A-780. Second,

[11] Stabile argues that his attempted revocation of Deetz's consent must be construed as a "request for re-possession of his seized property. Appellant's Br. 26. We disagree. In response to the officers' statement to Stabile that Deetz had already given consent to a search of the house, Stabile replied, "I take it back." This bare statement cannot be transformed into a request for return of the hard drives. Moreover, Stabile concedes, as he must, that our opinion in *United States v. King* forecloses his attempt to revoke consent pursuant to *Georgia v. Randolph*. Appellant's Br. 35 n.16.

although Stabile claims he needed a computer for work, Deetz brought a replacement computer to the house one day after Stabile's computers had been seized. *Appx*. at A-473-75.

We also consider the Government's rationale for the delay. Agent Albanese testified that the three-month delay in securing a state search warrant was due to his assignment to a Secret Service Detail protecting the President and other high officials. Moreover, because Albanese was the lead case agent, he was responsible for seeking the state search warrant. Stabile notes that the Eleventh Circuit in *Mitchell* rejected the argument that a 21-day delay was not unreasonable because the officer was attending a training seminar. *Mitchell*, 565 F.3d at 1352. However, the *Mitchell* court explicitly stated that "we emphasize that we are applying a rule of reasonableness that is dependent on all of the circumstances." *Id*. Moreover, the *Mitchell* court stated that it would be "sympathetic" if "some overriding circumstances arose, necessitating the diversion of law enforcement personnel to another case." *Id*. at 1353. Here, such overriding circumstances were present because Agent Albanese was assigned to what was obviously important security work. Agent Albanese was also the lead investigator on a multiple-county investigation requiring coordination. Considering this explanation along with the other factors, we believe the Government's three-month delay in obtaining a state search warrant was reasonable under the circumstances. Nevertheless, the delay was not unavoidable, and we are troubled by it. In the absence of the same circumstances present here, we might very well reach a different result.

III.A.4. Execution of State Search Warrant

As previously discussed, Agent Albanese obtained the state search warrant on October 19, 2006. In mid-November, Detective Vanadia commenced a warranted search of the 120 GB hard drive solely for evidence of financial crimes.[12] During this search, Vanadia noticed a folder named "Kazvid." The folder contained files bearing names indicative of child pornography. Vanadia then opened these files and "confirmed" that they did contain child pornography. Stabile argued that this search violated the Fourth Amendment and that the fruits of the search had to be suppressed.

The District Court first determined that Detective Vanadia lawfully opened the Kazvid folder. The District Court then found that the *file names* of the files in the Kazvid folder were in "plain view," but that the plain view doctrine did not encompass the *contents* of those files. However, the District Court determined that Vanadia's decision to view the contents of the files, although violative of the Fourth Amendment, did not require suppression because of the inevitable discovery doctrine.

On appeal, Stabile challenges each step of this search, arguing that: (1) Detective Vanadia improperly opened the

[12] The warrant initially authorized a search for evidence of *both* financial crimes and child pornography. However, because probable cause was based on DVDs found in Stabile's desk that did not actually contain child pornography, the District Court determined that the child pornography section of the warrant had to be excised in violation of *Franks v. Delaware*, 438 U.S. 154 (1978). *United States v. Stabile*, 2009 U.S. Dist. LEXIS 4263, at *20-*21 (D.N.J. Jan. 21, 2009). The parties do not dispute this decision.

"Kazvid" folder; (2) that the plain view doctrine should not apply to the file names found in the Kazvid folder; and (3) that the inevitable discovery and independent source doctrines do not apply and therefore this evidence must be suppressed. The Government contends that the plain view doctrine applies not only to the names of the files in the Kazvid folder but also to all the contents of those files. For the reasons that follow, we determine that Detective Vanadia properly opened that Kazvid folder; that the names of the files in that folder were in plain view; and that although under the facts of this case the plain view doctrine may not apply to the contents of those files, the independent source and inevitable discovery doctrines apply to the contents of the files, thereby removing any need for suppression. Therefore, we will affirm the District Court's decision.

III.A.4.a. View of Files in "Kazvid" Folder

The first issue is whether, pursuant to the state search warrant to search for evidence of financial crimes, Detective Vanadia properly viewed the files in the Kazvid folder. The District Court found that Vanadia properly opened this file because he reasonably believed that it could contain evidence of financial crimes.

Stabile contends that Detective Vanadia "stumbled" upon the videos in the Kazvid folder by failing to limit the scope of his search to evidence of financial crimes. Appellant's Br. 29. According to Stabile, Vanadia's decision to open Kazvid was an unreasonably overbroad search, not limited to evidence of financial crimes, and a pretext for searching for child pornography. *See* Appellant's Br. 29-30, 37 n.19. We disagree.

Resolution of this issue forces us 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. *See United States v. Burgess*, 576 F.3d 1078, 1092-94 (10th Cir. 2009) ("[T]here may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders, and that is true whether the search is of computer files or physical files."); *United States v. Mann*, 592 F.3d 779, 782 (7th Cir. 2010) (relevant files are often hidden and can be mislabeled and "manipulated to hide their true contents"); *Adjani*, 452 F.3d 1140, 1150 (9th Cir. 2006). On the other hand, as Stabile argues, granting the Government a *carte blanche* to search *every* file on the hard drive impermissibly transforms a "limited search into a general one." *Marron v. United States*, 275 U.S. 192, 196 (1927) ("The requirement that warrants shall particularly describe things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another."); *see United States v. Tracey*, 597 F.3d 140, 146 (3d Cir. 2010). To reconcile these competing aims, many courts have suggested various strategies and search methodologies to limit the scope of the search.

In *United States v. Comprehensive Drug Testing, Inc.*, the federal government investigated the Bay Area Lab Cooperative ("Balco"), suspected of providing steroids to professional baseball players. 621 F.3d 1162, 1166 (9th Cir. 2010). In 2002, the Major League Baseball Players Association entered into a collective bargaining agreement

that provided for drug testing of all players (performed by Comprehensive Drug Testing) for the purpose of determining only whether more than five percent of players tested positive. *Id*. The players were assured that the results would remain anonymous and confidential. *Id*. During the Balco investigation, the government learned of ten players who had tested positive, and it sought and obtained a warrant limited to the records of ten players as to whom there was probable cause to search. *Id*. However, when the government executed the warrant, the government seized and reviewed the drug testing record for *hundreds* of players. *Id*. On appeal to the Ninth Circuit *en banc*, the *en banc* court discussed proper procedures for handling seized data premised on its earlier opinion in *Tamura*. *Id*. At 1167. For example, the initial review and segregation of the data was to be performed not by the case agents but by "law enforcement personnel trained in search and seizing computer data." *Id*. At 1168. The government was to return any data that did not fall within the scope of the warrant. *Id*. At 1168-69. As the Ninth Circuit stated:

> We recognize the reality that over-seizing is an inherent part of the electronic search process and proceed on the assumption that, when it comes to the seizure of electronic records, this will be far more common than in the days of paper records. This calls for greater vigilance on the part of judicial officers in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures. The process of segregating electronic data that is seizable from that which is not must

> not become a vehicle for the government to gain access to data which it has no probable cause to collect.

Id. At 1177.

In *United States v. Carey*, the Tenth Circuit suggested methods to avoid searching files of the type not identified in the warrant, such as "observing files types and titles listed on the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory." 172 F.3d 1268, 1276 (10th Cir. 1999). The Tenth Circuit has refined its approach since *Carey*. In *Burgess*, the Tenth Circuit considered the appropriate standards for searching a hard drive, offering the following guidance: "while officers must be clear as what it is they are seeking on the computer and conduct the search in a way that avoids searching files of types not identified in the warrant," *United States v. Walser*, 275 F.3d 981, 986 (10th Cir. 2001), "a computer search may be as extensive as reasonably required to locate the items described in the warrant" based on probable cause. *United States v. Grimmett*, 439 F.3d 1263, 1270 (10th Cir. 2006) (quotations omitted). But the search warrant itself need not "contain a particularized computer search strategy." *United States v. Brooks*, 427 F.3d 1246, 1251 (10th Cir. 2005). Given that it would be "folly for a search warrant to structure the mechanics of the search" because "imposing such limits would unduly restrict legitimate search objectives," *Burgess*, 576 F.3d at 1094, the scope of the search must be "constrained by content." *Id*. at 1093. In *Burgess*, that content was computer files containing evidence of drug use or trafficking. *Id*. To avoid transforming a limited search into a general one, the court cautioned that "[a]s the description of

such places and things becomes more general, the method by which the search is executed become[s] more important – the search method must be tailored to meet allowed ends." *Id*. at 1094. Speaking directly to search methodology, *Burgess* recommended that computer searches begin by using search protocol to structure the search with an analysis of the file structure, followed by a search for suspicious file folders, and then looking for files and types of files most likely to contain the objects of the search by doing keyword searches. *Id*. In the end, however, the *Burgess* court noted that "there may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders . . . ." *Id*.

Finally, in *United States v. Mann*, the defendant argued that the government's search of his computer for evidence of voyeurism exceeded the scope of the search warrant where the search produced evidence of child pornography. 592 F.3d at 781. The Seventh Circuit held that the search was lawful, and noted the particular difficulties in attempting to locate image files on a computer because the files may be "manipulated to hide their true contents." *Id*. at 782; *see Hill*, 459 F.3d at 978 ("Images 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.").

Turning to the instant case, the scope of the consent and state search warrant were limited to evidence of financial crimes. For a number of reasons, we believe that Detective Vanadia's decision to highlight and view the contents of the

Kazvid folder was reasonable and permissible under the Fourth Amendment.

First, Detective Vanadia's decision to highlight and view the contents of the Kazvid folder was objectively reasonable because criminals can easily alter file names and file extensions to conceal contraband. *See Williams*, 592 F.3d at 522; *Hill*, 459 F.3d at 978. Second, Detective Vanadia's search procedures complied with the search procedures outlined in *Carey* – a case which advocates more restrictive search procedures than the broader search procedures approved in *Williams* and *Burgess*. For example, *Carey* suggested search methods such as focusing on the file type identified in the warrant, file names, key word search, and directory structure. 172 F.3d at 1276. Conversely, *Williams* stated that a computer search authorized at least a "cursory review of each file on the computer." 592 F.3d at 522. Likewise, *Burgess* suggested that "there may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders" while conducting an electronic search. 576 F.3d at 1094. Here, Vanadia took steps to ensure that his investigation complied with the state search warrant. Vanadia began by physically inspecting the hard drive and creating a copy of the drive to ensure that the original drive was not damaged or corrupted during the search. Next, Vanadia examined the file signatures to see if any files had been corrupted. He then conducted a "hash value analysis" to see if any files had been copied. Finally, he examined suspicious and out-of-place folders, such as the Kazvid folder. *Appx*. at A-521-27, A-531-32, A-536-37. These procedures

demonstrate that Vanadia engaged in a focused search of the hard drives rather than a general search.[13]

Finally, Stabile argues that Detective Vanadia exceeded the scope of the state search warrant because Vanadia testified that he knew that there *may* have been child pornography contained in the Kazvid folder.[14] This argument

---

[13] We note that although Stabile argues that Detective Vanadia's search methodology was overbroad, Stabile offers no practical alternative methodology that would have protected his interests yet still permitted a thorough search for evidence of financial crimes. *See Burgess*, 576 F.3d at 1095; *Brooks*, 427 F.3d at 1251. Indeed, Stabile's only suggestion was for Vanadia to use EnCase software to conduct a "green home plate highlighting of the entire hard drive," which would have permitted Vanadia to isolate file types. Appellant's Br. 28. But because evidence of check fraud is often contained on image files, if Vanadia *had* employed Stabile's suggested method, he still would have isolated image files and, eventually, Vanadia would have discovered images of child pornography. Therefore, Stabile fails to propose a legitimate alternative methodology.

[14] Stabile quoted the following testimony in support of his argument:

> Q. At the moment that you were making the decision to open up Kazvid, didn't you say to yourself, you know, there may well be child pornography here?
> A. Sure.
> Q. Okay. So it's not true that you opened the folder only for the purpose of trying to see whether or not

fails because an investigator's subjective intent is not relevant to whether a search falls within the scope of a search warrant. *See Maryland v. Garrison*, 480 U.S. 79, 84 (1987) ("the scope of a lawful search is defined by the object of the search and the places in which there is probable cause to believe it may be found") (internal citation omitted); *Williams*, 592 F.3d at 524 (where investigators executed search warrant for evidence of computer harassment on defendant's hard drive, plain view seizure of child pornography discovered during search was permissible "even if finding child pornography was their hope from the outset").[15] Here, the state search warrant objectively authorized Vanadia to search for evidence of financial crimes, and Vanadia's testimony that he subjectively believed the Kazvid folder *could* harbor evidence of child pornography does not render the search of the Kazvid folder invalid. Moreover, as Vanadia made clear in his testimony, the Kazvid folder required further investigation because evidence of financial crimes could be hidden within. *Appx*. at A-536-37.

> there were financial crimes or evidence of financial crimes lurking in the Kazvid directory. Isn't that fair to say?
> A. Yes.

Appx. at A-42.

[15] *See also Horton v. California*, 496 U.S. 128, 138 (1990) ("The fact that an officer is interested in an item of evidence and fully expects to find it in the course of a search should not invalidate its seizure if the search is confined in an area and duration by the terms of a warrant or a valid exception to the warrant requirement.").

For the foregoing reasons, we conclude that highlighting the Kazvid folder was reasonable and did not exceed the scope of the state search warrant.

III.A.4.b. Plain View Examination of File Names

After highlighting the Kazvid folder, Detective Vanadia observed in the folder a list of files with lurid names. The Government argues that these file names may be examined pursuant to the plain view doctrine. Stabile disagrees. This brings us to the question of whether evidence of other crimes in a computer can be examined under the plain view doctrine. We hold that the plain view doctrine applies to seizures of evidence during searches of computer files, but the exact confines of the doctrine will vary from case to case in a common-sense, fact-intensive manner.[16]

[16] We decline to follow the Ninth Circuit's suggestion to "forswear reliance on the plain view doctrine" whenever the government seeks a warrant to examine a computer hard drive. *United States v. Comprehensive Drug Testing*, 621 F.3d 1162, 1178 (9th Cir. 2010) (Kozinski, C.J., concurring). Instead, we agree with the Seventh Circuit's view that rather than jettisoning the plain view doctrine entirely in electronic searches, "the more considered approach 'would be to allow the contours of the plain view doctrine to develop incrementally through the normal course of fact-based adjudication.'" *Mann*, 592 F.3d at 785 (quoting *Comprehensive Drug Testing*, 621 F.3d at 1184 (Callahan, J., concurring in part and dissenting in part from the en banc panel's per curiam opinion)). In short, we agree that "[a] measured approach based on the facts of a particular case is

What is permissible in one situation may not always be permissible in another.

There are three requirements for valid seizures of evidence in plain view. "First, the officer must not have violated the Fourth Amendment in 'arriving at the place from which the evidence could be plainly viewed.' Second, the incriminating character of the evidence must be 'immediately apparent.' Third, the officer must have 'a lawful right of access to the object itself.'" *United States v. Menon*, 24 F.3d 550, 559-60 (3d Cir. 1994) (quoting *Horton*, 496 U.S. at 141) (internal citations omitted). Detective Vanadia's examination of the file *names* in the Kazvid folder, to the extent that he may arguably be said to have "seized" the names by, for example, making a screen print, satisfies all three plain view requirements.[17]

---

especially warranted in the case of computer-related technology, which is constantly and quickly evolving." *Comprehensive Drug Testing*, 621 F.3d at 1184 (Callahan, J., concurring in part and dissenting in part from the *en banc* panel's per curiam opinion). We engage in just such a fact-intensive inquiry here.

[17] Mere observation must be distinguished from seizure, a distinction that may become hazy in the digital environment. We do not believe that simply seeing the file names constitutes a seizure. *See Texas v. Brown*, 460 U.S. 730, 739 n.4 (1983) (plurality opinion) ("It is important to distinguish 'plain view,' . . . to justify *seizure* of an object, from an officer's mere observation of an item left in plain view. Whereas the latter generally involves no Fourth Amendment search . . . , the former generally does implicate the

First, Detective Vanadia did not violate the Fourth Amendment in arriving at the place from which the evidence could be viewed. Deetz consented to the seizure of all six hard drives and a magistrate issued a state search warrant to search all six hard drives for evidence of financial crimes. Vanadia began executing the state search warrant by searching the 120 GB hard drive. Within the 120 GB hard drive, Vanadia noticed the Kazvid folder. He lawfully highlighted the Kazvid folder to view its contents because a thorough computer search requires a broad examination of files on the computer to ensure that file names have not been manipulated to conceal their contents. *See Williams*, 592 F.3d at 522; *Hill*, 459 F.3d at 978. Nor did Vanadia unreasonably expand the scope of his search by highlighting the Kazvid folder and viewing its contents. *See Mann*, 592 F.3d at 784 (search was lawful where investigator conducted search within scope of warrant and did not knowingly expand the scope of the search to discover child pornography). Therefore, the first plain view requirement is satisfied because Vanadia "lawfully arrived at the point from which the evidence could be viewed."

Amendment's limitations upon seizures of personal property. The information obtained as a result of observation of an object in plain sight may be the basis for probable cause or reasonable suspicion of illegal activity. In turn, these levels of suspicion may, in some cases, . . . justify police conduct affording them access to a particular item.") (internal citations omitted). Whether recording the names in some fashion implicates the Fourth Amendment is not something we need to decide in this case. We will assume that it does, solely for the sake of analyzing why Stabile's arguments fail.

Second, there is no doubt that the incriminating character of the evidence—in this instance the names themselves—was "immediately apparent."[18] The Kazvid folder contained files with lurid names. These file names suggested that Stabile illegally possessed contraband (child pornography). *See Williams*, 592 F.3d at 522 ("[W]hen the officer then comes upon child pornography, it becomes 'immediately apparent' that its possession by the computer's owner is illegal and incriminating.").

Third, Detective Vanadia had a "lawful right of access" to the object of the search because he was authorized by a state search warrant to search the 120 GB hard drive for evidence of Stabile's financial crimes. *See id.*

Therefore, we conclude that the Government properly examined the file *names* listed in the Kazvid folder pursuant to the plain view doctrine.

III.A.4.c. Plain View Examination of File Contents

After highlighting the Kazvid folder, Detective Vanadia viewed a list of file names with file extensions suggesting child pornography videos. Vanadia testified that

[18] Again, it is only because the file names themselves have evidentiary significance and may at least arguably be "seized" via, for example, a screen print, and then tendered in evidence, that the plain view doctrine could be implicated at all. *See Brown*, 460 U.S. at 739 n.4 (distinguishing "plain view" as a doctrine that justifies the seizure of evidence from the mere observation of things in plain sight).

he opened these video files to "confirm" they contained child pornography. *Appx*. at A-534-35, A-591-92. The Government claims in their brief that under the plain view doctrine, once Detective Vanadia saw the lurid file names he was then empowered to seize and examine the contents of those files. Gov't's Br. 38. Stabile argues, and the District Court concluded, that opening the video files to view their contents exceeded the scope of the state search warrant and that plain view did not apply, resulting in an illegal search.[19] The state search warrant issued on October 19, 2006 authorized Vanadia to search all six hard drives only for evidence of financial crimes.[20]

We need not resolve whether the plain view doctrine applies to examination of contents of the video files because the independent source and inevitable discovery doctrines apply to the contents of all the video files. Therefore, we ultimately conclude that suppression is not required.

III.A.4.d. Independent Source

[19] The District Court concluded, however, that this violation did not require suppression because the inevitable discovery doctrine applied.

[20] The warrant also authorized a search for child pornography in the DVDs found in a desk in Stabile's home. These DVDs did not contain child pornography, and the District Court ultimately excised this portion of the warrant because it ran afoul of *Franks v. Delaware*. *Appx*. at A-101.

Even assuming Detective Vanadia illegally opened and examined the contents of the video files in the Kazvid folder, the independent source doctrine applies and removes any taint from this search.[21] Typically, the exclusionary rule requires that we suppress evidence obtained as a result of an illegal search. *Wong Sun v. United States*, 371 U.S. 471, 485 (1963). However, "[t]he independent source doctrine serves as an exception to the exclusionary rule and permits the introduction of 'evidence initially discovered during, or as a consequence of, an unlawful search, but later obtained independently from activities untainted by the initial illegality.'" *United States v. Price*, 558 F.3d 270, 281 (3d Cir. 2009) (quoting *Murray v. United States*, 487 U.S. 533, 537 (1988)). Here, the District Court concluded that suppression was not required because the inevitable discovery exception to the exclusionary rule applied.[22] For the reasons

---

[21] For purposes of applying the independent source doctrine, we assume, without deciding, that Vanadia illegally viewed the contents of the video files in the Kazvid folder.

[22] Following the District Court's January 21, 2009 order denying his motion to suppress, Stabile filed a motion to reconsider, arguing that the District Court erred by applying the inevitable discovery doctrine rather than the independent source doctrine. On March 13, 2009, the District Court denied Stabile's motion to reconsider and reaffirmed its reliance on the inevitable discovery doctrine. The District Court concluded that suppression was unnecessary under the independent source doctrine as well.

Here, we think the independent source doctrine more appropriately applies to the contents of the video files. We also think that the inevitable discovery doctrine applies to the

evidence obtained while executing the invalid first and second federal warrants, which were obtained subsequently.

The Third Circuit contrasted these doctrines in *United States v. Herrold*:

> [U]nder the independent source doctrine, evidence that was *in fact* discovered lawfully, and not as a direct or indirect result of illegal activity, is admissible. In contrast, the inevitable discovery doctrine, applied in *Nix*, permits the introduction of evidence that *inevitably would have* been discovered through lawful means, although the search that actually led to the discovery of the evidence was unlawful. The independent source and inevitable discovery doctrines thus differ in that the former focuses on what actually happened and the latter considers what would have happened in the absence of the initial search.

962 F.2d 1131, 1140 (3d Cir. 1992). Here, pursuant to the state search warrant, Vanadia *lawfully* discovered evidence of child pornography (lurid file names and the first video file) while searching for evidence of financial crimes. Although Vanadia may have exceeded the scope of the state search warrant by expanding the search and opening the contents of the video files, the initial inspection and resulting discovery were lawful. Accordingly, the independent source doctrine applies. In contrast, and for reasons we will discuss, the inevitable discovery doctrine applies to the ensuing *unlawful* searches made pursuant to the two federal search warrants.

that follow, we conclude that the independent source doctrine applies to the results of the search executed pursuant to the state search warrant and vitiates any need to suppress evidence of child pornography.

Assuming that Detective Vanadia illegally viewed the contents of the videos in the Kazvid folder, we ask whether this illegal search is so intertwined with the eventual acquisition of child pornography from Stabile's hard drives that this evidence must be suppressed. We ask: "(1) whether a neutral justice would have issued the search warrant even if not presented with information that had been obtained during an unlawful search and (2) whether the first search [the search of the contents of the eleven video files] prompted the officers to obtain the [subsequent] search warrant." *Herrold*, 962 F.2d 1131, 1144 (3d Cir. 1992); *see Price*, 558 F.3d at 282. "If the answers to these questions are yes and no respectively . . . then the evidence seized during the warranted search, even if already discovered in the original entry, is admissible." *Herrold*, 962 F.2d at 1144.

The answer to the first question is "yes." After Detective Vanadia executed the state search warrant, Agent Albanese applied for the first federal search warrant. The application for the first federal search warrant cited, as probable cause, the lurid file names Vanadia observed in plain view during his search of the 120 GB hard drive. The application also cited Vanadia's experience that files bearing such names may contain child pornography. Importantly, the warrant application did not mention that Vanadia had viewed

---

These subsequent searches were unlawful for lack of probable cause.

the contents of *any* of the video files.[23] Even assuming that Vanadia illegally viewed the video files' contents, the results of that search did not taint the warrant application Albanese presented to the magistrate. *See Price*, 558 F.3d at 282 (applying independent source doctrine where warrant was still supported by probable cause even after excising illegally-obtained information). After considering the warrant application, the magistrate issued the first federal search warrant. Therefore, the answer to the first inquiry under the independent source doctrine is clearly yes because a neutral magistrate did, in fact, issue the first federal search warrant.

The answer to the second question is "no." The contents of the video files, which we presume Detective Vanadia viewed illegally, did not prompt Agent Albanese to apply for the first federal search warrant. In *Price*, police arrested the defendant after he sold methamphetamine to an undercover police officer. 558 F.3d at 273. A search incident to the arrest "revealed items indicative of methamphetamine trafficking." *Id*. The police then went to the defendant's home, where they asked for, and received, consent to search the home from the defendant's wife. *Id*. at 274. After searching the home, the police attempted to obtain consent to search the locked basement, but the defendant's wife said she did not have a key. *Id*. at 275. The officer picked the lock on the basement door, entered the basement, and observed items used to manufacture methamphetamine. *Id*. Later that day, police applied for and obtained a search warrant, returned to the home, and seized the chemicals related to methamphetamine manufacture from the basement. *Id*. The defendant moved to suppress the items seized from the

[23] The full text of the affidavit is contained in footnote 6.

basement on the grounds that the police lacked valid consent to enter the basement, and the district court denied the relevant portion of the motion. *Id*. at 276. On appeal, we held that regardless of the validity of the wife's consent, the items seized from the basement were admissible under the independent source doctrine. *Id*. at 280. First, the illegally observed evidence did not prompt the officers to apply for the search warrant. *Id*. at 282. Second, the search warrant contained sufficient probable cause from independent sources even though the affidavit in support of the warrant application referenced the items illegally discovered in the basement. *Id*. Even without this evidence, given the history of the investigation, such as the facts that the defendant had incriminating paraphernalia on his person at the time of arrest and that paraphernalia was found in his home, it seemed "impossible that the police would not have applied for a warrant to search the basement of the house . . . ." *Id*. at 282; *see also Herrold*, 962 F.2d at 1140-41 ("It is inconceivable that the police would have Justified the premises without searching the trailer and without arresting [the defendant] since they had information that Herrold, who was known to them as a drug dealer with a record of convictions for violent crimes, had obtained a large quantity of cocaine some of which he sold to the informant."). Therefore, the *Price* court invoked the independent source doctrine and affirmed the district court's suppression order.

Here, there are even more compelling reasons to vitiate the taint of the presumed illegal search than existed in *Price*. In *Price*, the search warrant application referenced the illegally observed evidence, but here, as previously mentioned, the warrant application made no mention of the contents of the Kazvid video files. This distinction supports

our determination that if the contents of the remaining video files were illegally viewed, they did not prompt Agent Albanese to seek the first federal search warrant. Moreover, as in *Price*, here the police legally discovered ample additional evidence. While executing the state search warrant, Detective Vanadia lawfully viewed lurid file names indicative of child pornography. In light of this evidence, it would be "impossible" or "inconceivable" that Albanese would not have applied for the first federal warrant. *See Price*, 558 F.3d at 282; *Herrold*, 962 F.2d at 1140. The answer to the second question in the independent source inquiry – *i.e.*, whether the results of the illegal search prompted officers to obtain a subsequent search warrant – is "no" because the lurid file names prompted Albanese to seek the first federal search warrant. Therefore, the independent source doctrine applies, and there would be no reason to suppress the contents of the videos.

III.A.4.e. Inevitable Discovery

The independent source doctrine removes the taint of any illegality from the initial search of the contents of the Kazvid folder in the 120 GB hard drive. However, the subsequent searches of the 120 GB hard drive and ultimately all the hard drives were illegal because these searches were not supported by valid warrants. As previously discussed, the first federal search warrant was invalid because it mistakenly authorized a search of the 40 GB hard drive rather than the 120 GB hard drive. The second federal search warrant was invalid because it relied on evidence obtained from the unlawful search of the 40 GB hard drive. Despite this illegality, the inevitable discovery doctrine applies, rendering

suppression of the evidence gathered as a result of these illegal searches unnecessary.

Under the inevitable discovery doctrine, "if the prosecution can establish by a preponderance of the evidence that the information ultimately or inevitably would have been discovered by lawful means . . . then the deterrence rationale has so little basis that the evidence should be received." *United States v. Vasquez De Reyes*, 149 F.3d 192, 195 (3d Cir. 1998) (quoting *Nix v. Williams*, 467 U.S. 431 (1984)). The Government can meet its burden by establishing "that the police, following routine procedures, would inevitably have uncovered the evidence." *Vasquez De Reyes*, 149 F.3d at 195. The inevitable discovery analysis focuses on "historical facts capable of ready verification, not speculation." *Id.*; *see Nix*, 467 U.S. at 444 n.5.

As the District Court concluded, the Government has shown by a preponderance of the evidence that routine police procedures inevitably would have led to the discovered child pornography. Although the first federal search warrant mistakenly called for searching the 40 GB hard drive rather than the 120 GB hard drive, the file names in the Kazvid folder Detective Vanadia opened still continued to provide probable cause to obtain a valid warrant to search the 120 GB hard drive. A lawful search of the 120 GB hard drive would have led to the videos of child pornography in the Kazvid folder. These videos, in turn, would have provided probable cause to obtain federal search warrants to search Stabile's five remaining hard drives for evidence of child pornography, including the illegally searched 40 GB hard drive.

This conclusion is supported by "historical facts capable of ready verification, and not speculation." *Vasquez De Reyes*, 149 F.3d at 195. As previously discussed, the Government lawfully obtained the state search warrant, and execution of the state search warrant exposed lurid file names and at least one video of child pornography. Thus, "viewing affairs as they existed at the instant before the unlawful search," *Vasquez de Reyes*, 149 F.3d at 195, the Government had probable cause to obtain a warrant to conduct a full search of the 120 GB hard drive. In accordance with routine police procedures, the Government attempted to obtain the first federal search warrant before fully searching the 120 GB hard drive. Moreover, the Government sought the second federal search warrant before embarking on a search of Stabile's five remaining hard drives. As the District Court found, "Albanese's application for the second federal search warrant [was] based on Agent Tokash's search of the 40 GB hard drive and the second federal search warrant issued based on probable cause supplied by the evidence discovered in Agent Tokash's search." *Appx*. at A-107-08. Although mistakes were made, proper execution of these routine procedures would have yielded evidence of child pornography. Moreover, the very fact that the Government attempted to secure state and federal search warrants at every step of the search indicates that there would be little deterrence benefit in punishing the Government. *See Vasquez De Reyes*, 149 F.3d at 195 (inevitable discovery doctrine "permits the court to balance the public interest in providing a jury with all relevant and probative evidence in a criminal proceeding against society's interest in deterring unlawful police conduct"). We conclude that the evidence obtained as a result of these illegal searches need not be suppressed because it inevitably would have been discovered.

III.B. Sentencing

Stabile also claims that his sentence is unreasonable. Because Stabile knowingly and voluntarily waived his right to appeal, and because nothing compels us to disregard this waiver, we decline to exercise our jurisdiction to review the merits of this claim.[24]

Prior to sentencing, Stabile agreed to a set of "non-jury trial stipulations," which included a waiver of the right to "challenge [on appeal] the sentence imposed . . . if that sentence falls within or below the Guidelines range that results from the agreed total Guidelines offense level of 26."[25] *Appx*. at A-74. Stabile was sentenced to 78 months' imprisonment, the bottom of the applicable Guidelines range. Moreover, our review of the record provides no indication that Stabile's waiver was anything less than knowing and voluntary. Waivers of appellate rights, if entered into knowingly and voluntarily, are valid. *See United States v. Khattak*, 273 F.3d 557, 562 (3d Cir. 2001).

Nonetheless, Stabile urges us to reach his claims by arguing that a constitutional concern and a procedural defect allegedly committed by the District Court amount to a

---

[24] We review *de novo* whether Stabile waived his right to appeal his sentence. *Price*, 558 F.3d at 277.

[25] Stabile did not waive his right to appeal determination of his criminal history category, but he does not dispute this calculation.

miscarriage of justice. In rare circumstances, we will exercise our jurisdiction irrespective of a waiver "where an error amount[s] to a miscarriage of justice." *Khattak*, 237 F.3d at 562; *see United States v. Gwinnett*, 483 F.3d 200, 203 (3d Cir. 2007). This exception "will be applied sparingly and without undue generosity." *United States v. Wilson*, 429 F.3d 455, 458 (3d Cir. 2005) (quoting *United States v. Teeter*, 257 F.3d 14, 26 (1st Cir. 2001)).

Stabile first argues that his sentence raises a "constitutional concern" because U.S.S.G. § 2G2.2, as amended, imposes increased punishment on individuals who merely possess child pornography based on congressional concerns relating solely to offenders who actually engage in pedophilia. *Appx.* at A-945-46. As acknowledged by the District Court, no evidence indicated that Stabile ever engaged in pedophilia. He thus argues that his sentence, imposed pursuant to U.S.S.G. § 2G2.2, punishes him for acts for which he has never been convicted, contrary to the tenets of *Apprendi v. New Jersey*, 530 U.S. 466 (2000). Stabile additionally argues that the District Court should have departed from the child pornography Guidelines because they are neither the product of empirical research nor consistent with the Sentencing Commission's characteristic institutional role, as recently acknowledged by the Third Circuit in *United States v. Grober*, Nos. 09-1318 & 09-2120, 2010 U.S. App. LEXIS 21980, at *41-42 (3d Cir. Oct. 26, 2010).

Neither of these claims compel us to set aside Stabile's waiver. Even if preceding amendments to U.S.S.G. § 2G2.2 were motivated by concerns pertaining specifically to acts of pedophilia rather than possession of child pornography alone, we do not believe this to be a sufficient reason to justify

disregarding Stabile's waiver. *See United States v. Lockett*, 406 F.3d 207, 212-14 (3d Cir. 2005) (upholding a valid waiver of appellate rights even in light of a subsequent holding by the Supreme Court that the pre-*Booker* regime under which appellant was sentenced was unconstitutional); *United States v. Rubbo*, 396 F.3d 1330, 1335 (11th Cir. 2005) ("[T]he right to appeal a sentence based on *Apprendi*/*Booker* grounds can be waived in a plea agreement."). Moreover, while the District Court was entitled to depart from the child pornography Guidelines for the reasons cited by Stabile, neither *Kimbrough v. United States*, 552 U.S. 85 (2007) nor our recent decision in *Grober*, 2010 U.S. App. LEXIS 21980, required the District Court to take this course when sentencing Stabile. Similarly, Stabile's reliance on *United States v. Olhovsky*, 562 F.3d 530 (3d Cir. 2009) is misplaced. In *Olhovsky*, the District Court made critical procedural errors and ignored expert testimony pertaining to the youthful offender's unique potential for rehabilitation – factors that are absent from the case before us. *Id.* at 551.

We similarly conclude that the procedural defects alleged by Stabile are insufficient to merit setting aside his appellate waiver. Stabile argues that the District Court committed a procedural error by failing to sentence him at the higher end of the recommended Guidelines range in accordance with the Guidelines provision applicable to combined offenses. U.S.S.G. § 3D1.4. Stabile also contends that the District Court erred by failing to adequately explain its rejection of his arguments in favor of a non-Guidelines sentence. Neither of these purported errors justify disregarding Stabile's waiver as we do not believe that they amount to a miscarriage of justice. *See United States v. Jackson*, 523 F.3d 234, 244 (3d Cir. 2008) ("[I]t will be a rare

and unusual situation when claims of an unreasonable sentence, standing alone, will be sufficient to invalidate a waiver because of a miscarriage of justice.").

Because we conclude that the sentence imposed by the District Court does not amount to a miscarriage of justice, we will not set aside Stabile's waiver and reach the sentencing challenges he presents on appeal.

IV.

We affirm the defendant's conviction and the District Court's denial of the motion to suppress. Because we will enforce the appellate waiver, we dismiss this sentencing appeal and thereby affirm the defendant's sentence.