ADVANCE SHEET HEADNOTE
October 26, 2015

2015 CO 60

No. 14SA281, People v. Herrera—Searches and Seizures—Criminal Law

The supreme court holds that neither the warrant permitting the police to search defendant Matthew Herrera's cellphone for indicia of ownership nor the plain view exception to the warrant requirement authorized the police to seize evidence of text messages between Herrera and a juvenile girl named Faith W. The warrant did not permit the police to search every folder in the phone for indicia of ownership because if it did, it would qualify as a general warrant in violation of the Fourth Amendment's particularity requirement. Furthermore, while the warrant authorizing a search for text messages between Herrera and "Stazi," the name used by an officer posing as a juvenile girl, rendered the police's initial intrusion into the text messaging application legitimate, and the incriminating nature of the particular folder they searched was immediately apparent under the circumstances, the third requirement of the plain view doctrine—that the police have lawful access to that folder's contents—was not met because there was no objective basis for the police to believe that it would contain messages from "Stazi." Accordingly, this court affirms the trial court's suppression of the evidence seized from the folder.

The Supreme Court of the State of Colorado
2 East 14th Avenue • Denver, Colorado 80203

2015 CO 60

Supreme Court Case No. 14SA281
Interlocutory Appeal from the District Court
Fremont County District Court Case No. 13CR322
Honorable Patrick W. Murphy, Judge

Plaintiff–Appellant:

The People of the State of Colorado,

v.

Defendant–Appellee:

Matthew James Herrera.

Order Affirmed
en banc
October 26, 2015

Attorneys for Plaintiff–Appellant:
Thom K. LeDoux, District Attorney, Eleventh Judicial District
Stacey L. Turner, Deputy District Attorney
Cañon City, Colorado

Attorneys for Defendant–Appellee:
Gillick & Wenner, P.C.
E. Michael Gillick
Cañon City, Colorado

JUSTICE EID delivered the Opinion of the Court.
CHIEF JUSTICE RICE dissents, and **JUSTICE BOATRIGHT** joins in the dissent.

¶1 In this interlocutory appeal, the People argue that evidence of text messages between defendant Matthew Herrera and a juvenile girl named Faith W.[1] were admissible under a warrant authorizing a search of his cellphone for indicia of ownership, and, in the alternative, under the plain view exception to the warrant requirement. We disagree and affirm the trial court's suppression order.

¶2 Faith W.'s mother told police that she believed Herrera was having sexual interactions with her daughter. Soon thereafter, Detective Robert Dodd started texting Herrera posing as "Stazi," a fourteen-year-old girl. Eventually these texts led to Herrera's arrest, at which time police seized Herrera's cell phone.

¶3 Detective Dodd obtained a warrant to search the cell phone for indicia of ownership and for texts between "Stazi" and Herrera. Pursuant to Detective Dodd's direction, Detective Patrick Slattery performed the search of the phone. The police department's usual practice was to search a cellphone using the Cellebrite Device, which searches the memory of the phone and lets the officers download certain data—for instance, text messages or internet history. Herrera's phone, however, was not compatible with the Cellebrite Device. Detective Slattery therefore had to search the phone by hand and photograph what he found. Detective Slattery first searched the phone's standard text messages and identified texts between "Stazi" and Herrera sent

[1] We typically identify children and victims of sexual assault by using their initials or an appropriate general descriptive term. Cf. C.A.R. 32(f) (requiring that briefs and other appellate documents protect the identity of sexual assault victims and minors in criminal cases and cases brought under Title 19). In this opinion, we have initialized the victim's last name but use her first name in order to facilitate an understanding of the circumstances surrounding the search of Herrera's cell phone.

from Detective Dodd's number. Then, while scrolling through one of the phone's other messaging applications, Detective Slattery saw a message folder labeled "Faith Fallout." He knew that the department had been investigating Herrera's involvement with Faith W., and he suspected that "Faith Fallout" was Faith W.'s persona. He could not view the messages, however, without clicking on the folder name. Detective Slattery clicked on the name and, upon reading the text messages, confirmed that they were from Faith W.

¶4 We first reject the People's argument that the "Faith Fallout" texts were obtained under the warrant's authorization to search for "indicia of ownership" of the cellphone. The People contend that they were entitled under the warrant to search the entire contents of the phone because, for example, every text contained in the phone had the possibility of identifying Herrera as the owner of the phone. Such an interpretation of the warrant, however, proves too much, as it would render the warrant a general warrant in violation of the Fourth Amendment's particularity requirement. See People v. Roccaforte, 919 P.2d 799, 802 (Colo. 1996) (describing a general warrant as one that permits "a general, exploratory rummaging in a person's belongings") (citation omitted) (internal quotation marks omitted).

¶5 Next, we conclude that the "Faith Fallout" texts do not fall within the plain view exception to the warrant requirement. Under that exception, three requirements must be met: (1) the government's initial intrusion must be legitimate, (2) the incriminating nature of the evidence must be immediately apparent, and (3) the government must have the right to lawfully access the object. People v. Gothard, 185 P.3d 180, 183 (Colo.

2008). The first requirement is met in this case because the search warrant allowed Detective Slattery to search the phone for texts between Herrera and "Stazi." He was therefore justified in searching through one of the phone's text messaging applications, and while doing so, he saw the folder name "Faith Fallout." The second requirement is also met. Given the allegations against Herrera involving Faith W., the likely criminal nature of the name "Faith Fallout" was immediately apparent to Detective Slattery.

¶6 The third requirement, however, is not met in this case, as Detective Slattery did not have lawful access to the contents of the "Faith Fallout" folder. The "Faith Fallout" folder was essentially a separate, closed container filled with text messages from a particular number. Under the warrant, Detective Slattery could search containers that might reasonably contain messages from "Stazi." As the trial court found, however, messages from "Stazi" could not have reasonably been found in the "Faith Fallout" folder, as the circumstances indicated that that folder likely contained communications with Faith W., not "Stazi," and there was no suggestion that Herrera had deceptively labeled his files to conceal evidence. We agree with the trial court and accordingly affirm the suppression order.

I.

¶7 The mother of a juvenile girl named Faith W. reported to the Fremont County Sheriff's Office that Herrera had had sexual interactions with her daughter.[2] The mother provided the officers with printouts of online conversations between Faith W. and Herrera as well as Herrera's cell phone number.

[2] The following comes from the trial court's suppression hearing record.

¶8 Using Herrera's number, Detective Dodd started texting Herrera posing as a fourteen-year-old girl called "Stazi." These texts led to Herrera's arrest several weeks later. During this arrest, officers seized the cell phone from Herrera. At no time did Herrera deny ownership of the phone.

¶9 Detective Dodd applied for and received a search warrant for the phone. The warrant allowed a search of the phone for (1) texts sent between Herrera and "Stazi," (2) photographs sent between Herrera and "Stazi" that were attached to text messages, and (3) indicia of ownership to show the phone belonged to Herrera.

¶10 Detective Dodd gave the phone to Detective Slattery to search. Detective Dodd told Detective Slattery the basic details of the case, including Faith W.'s name, "Stazi's" phone number, and the suspected communications between "Stazi" and Herrera.

¶11 The police department's usual practice for searching cell phones was to use an instrument called the Cellebrite Device. This instrument searches the memory of the phone and lets the officers download certain data—for instance, text messages and internet history. Herrera's phone, however, was not compatible with the Cellebrite Device. Detective Slattery therefore had to search the phone by hand and photograph what he found.

¶12 Detective Slattery first went through the phone's standard text messages. Because the standard messages were arranged chronologically rather than by name, he had to scroll through all of the messages to find the entire conversation. He discovered several messages between "Stazi" and Herrera sent from Detective Dodd's number.

¶13 After going through all the standard text messages, he looked through the messages on the phone's Kik application. Kik is another method of sending messages—it simply sends them over the internet rather than the cellular network. The messages in Kik were organized by name. While scrolling to find more messages between Herrera and "Stazi," Detective Slattery found a text message folder identified by the name "Faith Fallout" that contained messages from a phone number other than Detective Dodd's. Detective Slattery knew the victim's name in the underlying case was Faith W. and that she and Herrera had been communicating digitally. Suspecting "Faith Fallout" was Faith W., Detective Slattery clicked on the name and found that it was the conversation between Faith W. and Herrera.

¶14 Herrera was charged with one count of sexual assault on a child,[3] one count of internet sexual exploitation of a child,[4] and one count of internet luring of a child.[5] Herrera filed a Motion to Suppress, inter alia, the texts between him and Faith W. found during Detective Slattery's search of the phone.

¶15 At the suppression hearing, Detective Slattery testified that he was given Detective Dodd's cell phone number and that he searched for texts between Herrera and "Stazi" associated with that number. Detective Slattery further testified that the "Faith Fallout" folder was associated with a number other than Detective Dodd's, and that he believed that the messages contained in the folder belonged to the victim in this

[3] § 18-3-405(1), C.R.S. (2015).

[4] § 18-3-405.4(1), C.R.S. (2015).

[5] § 18-3-306(1), (3), C.R.S. (2015).

case, Faith W. Finally, Detective Dodd testified that there was no connection between his number and the number belonging to "Faith Fallout."

¶16 The trial court granted the motion and suppressed the texts between "Faith Fallout" and Herrera. The court found that Detective Slattery could not have reasonably concluded that the "Faith Fallout" folder would contain messages from "Stazi" because there was no link between that folder and Detective Dodd's number. The trial court thus concluded that Detective Slattery exceeded the scope of the warrant by clicking on the name to look at the messages. It also held that none of the exceptions to the warrant requirement applied. The People appealed that ruling to this court under C.A.R. 4.1.[6]

II.

¶17 The People argue that the text messages contained in the "Faith Fallout" folder were admissible under the search warrant issued in this case, and, in the alternative, under the plain view exception to the warrant requirement. We address each argument in turn.

A.

¶18 The warrant in this case authorized a search of Herrera's cellphone for text messages between Herrera and "Stazi" as well as for "indicia of ownership." The

[6] The People also filed a certificate pursuant to section 16-12-102(2), C.R.S. (2015), stating that the text messages constitute a "substantial part of the proof of the charge pending against the defendant" because they are direct communications between an alleged victim and a defendant charged with "entic[ing] through . . . a text message or instant message, a person whom the actor knows or believes to be under fifteen years of age." § 18-3-405.4(1).

People contend that the warrant thus permitted a search of the text messages contained in the "Faith Fallout" folder because any message found there would reveal Herrera as the owner of the phone. We believe this argument proves too much, as it would authorize a general search of the entire contents of the phone. Indeed, the People argue that any piece of data on the phone, including any text message on the phone, would have the possibility of revealing Herrera's ownership of the phone. This rationale transforms the warrant into a general warrant that fails to comply with the Fourth Amendment's particularity requirement.

¶19 The Warrant Clause of the Fourth Amendment requires that a warrant "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. The particularity requirement is designed to "prevent officers from conducting a 'general, exploratory rummaging in a person's belongings.'" Roccaforte, 919 P.2d at 802 (citing Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971)). As the U.S. Supreme Court recently observed, "the Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." Riley v. California, ___ U.S. ___, 134 S. Ct. 2473, 2494 (2014). In this case, the People's rationale would permit officers to "rummage through" the entirety of an individual's private information contained in his phone, without limitation.

¶20 To be sure, this court has sustained some fairly broad searches against particularity challenges. For example, in Roccaforte, we reversed the trial court's

suppression of evidence stemming from a search pursuant to a warrant that permitted a search for all records pertaining to a business, including electronically stored data. 919 P.2d at 801–02. We held, however, that the warrant had to be read in conjunction with the supporting affidavit, which narrowed the search to business documents pertaining to particular dates that were related to a particular alleged crime. Id. at 804. Here, by contrast, the People's argument—namely, that they could search any and all data contained in Herrera's cell phone because any and all data could reveal his ownership of the phone—contains no such limits, or any limits.

¶21 Moreover, in Roccaforte, we noted that the breadth of the warrant was necessary in that case because the government had been unable to perform an audit of the business. Id. Here, again by contrast, such a necessity did not exist; in fact, the phone was seized from Herrera during his arrest, and he never disputed ownership of the phone.

¶22 In sum, we reject the People's argument that the search of the "Faith Fallout" folder was authorized by the warrant because such an argument is inconsistent with the particularity requirement.[7]

B.

¶23 The People argue in the alternative that the texts contained in the "Faith Fallout" folder could be searched under the plain view exception to the warrant requirement,

[7] On the same grounds, we reject the People's contention that the search was performed in good faith reliance upon the warrant and that therefore the good faith exception to the warrant requirement applies. See United States v. Leon, 468 U.S. 897, 923 (1984) (good faith exception does not apply where warrant "fail[s] to particularize the place to be searched or the things to be seized").

which holds that officers need not "close their eyes" to evidence of criminal activity in plain sight while they are conducting a lawful search. People v. Dumas, 955 P.2d 60, 63 (Colo. 1998). Here, the People argue that because Detective Slattery observed the "Faith Fallout" folder while he was searching for the "Stazi" texts, the folder could be opened and searched. We conclude, however, that the "Faith Fallout" folder is analogous to a closed container that could not reasonably contain texts between "Stazi" and Herrera, and that therefore the plain view exception does not apply.

¶24 Following the lead of the Supreme Court in Horton v. California, 496 U.S. 128, 136–37 (1990), this court has identified three requirements for applying the plain view exception to warrantless searches: (1) the government's initial intrusion must be legitimate, (2) the incriminating nature of the evidence must be apparent immediately, and (3) the government must have the right to lawfully access the object. Gothard, 185 P.3d at 183.

¶25 The search meets the first requirement that the initial intrusion be legitimate. Detective Slattery had a warrant to search the phone for messages between Herrera and "Stazi." Because the Kik application is used to send messages, it was reasonable for him to look for the messages there. It was during a search of the Kik application that he found the folder identified by the name "Faith Fallout." His initial intrusion was therefore legitimate.

¶26 The second requirement is also met, because the incriminating nature of the name was immediately apparent. To meet the second requirement, the police must have probable cause that the evidence is incriminating. People v. Pitts, 13 P.3d 1218,

1222 (Colo. 2000). In the context of a plain view seizure, "probable cause" requires "that the facts available to the officers would warrant a person of reasonable caution in the belief that certain items are contraband, fruits or instrumentalities of a crime, or evidence of criminal activity." People v. Melgosa, 753 P.2d 221, 227 (Colo. 1988). The concept, however, is incapable of having a precise definition and is instead dependent on "the totality of the circumstances." People v. Gutierrez, 222 P.3d 925, 937 (Colo. 2009) (citing Maryland v. Pringle, 540 U.S. 366, 371 (2003)). This court has enumerated two considerations necessary for probable cause: (1) "a reasonable ground for belief of guilt," and (2) that belief is "particularized with respect to the person to be searched or seized." Id. (citing Pringle, 540 U.S. at 371).

¶27 Our prior case law provides two relevant examples of analyzing probable cause for a plain view seizure. In People v. Najjar, 984 P.2d 592, 596–97 (Colo. 1999), this court addressed whether police officers had probable cause to examine and seize a luggage ticket in plain view during a legitimate search of a defendant's hip bag after a suitcase filled with marijuana was found at a bus station stop. In determining that the officers had probable cause to seize the luggage ticket, this court emphasized all of the facts the officers knew at the time. See id. For instance, the bag's ticket said it was going from Las Vegas to Detroit, and the defendant was the only person on the bus with that itinerary. See id. at 597. The defendant bought the bus ticket with cash using a fake name. Id. The defendant was very nervous. Id. Each luggage tag was unique, and the owner of the luggage would have the matching tag. Id. Finally, because the defendant denied having any luggage on the bus, he should not have had a luggage ticket to begin

with. Id. All of these separate facts, known to the officers at the time of the search, were enough probable cause to justify the plain view search and seizure of the luggage ticket. Id.

¶28 Dumas, 955 P.2d at 62, provides another example of probable cause for plain view seizures. Police officers were conducting a legitimate search of the defendant's motel room for drugs, weapons, and contraband. Id. During this, they searched through a checkbook and seized it as evidence of forgery. Id. This court ruled that the officers had probable cause to read through the checkbook and seize it because of the totality of what the officers knew at the time. Id. at 64. For instance, the court noted that (1) the checkbook was found beneath a mattress, and the checks were signed with a name other than the defendant's; (2) the officers found stamps worth over $1,000 in a shoebox, which the defendant claimed were a gift; and (3) receipts in the checkbook with the defendant's name showed she had returned over $1,000 worth of stamps to the post office. See id. Taken together, these facts created enough probable cause to seize the checkbook as evidence of forgery. Id.

¶29 As with Najjar and Dumas, this case is determined by a consideration of the facts known at the time of the search. In particular, we note the following facts that Detective Slattery knew at the time of his search. First, the name of the victim in the underlying case was Faith W. Second, Faith W. was communicating with Herrera digitally. Third, the name "Faith Fallout" was highly suggestive of Faith W. The name "Faith" was the same as the alleged victim's, while "Fallout" strongly suggested a false persona. Taken as a whole, these facts establish "a reasonable ground for belief" that the texts were

related to a crime, and these facts were particularized to Slattery's knowledge of Herrera and Faith W. See Gutierrez, 222 P.3d at 937. The incriminating nature of the "Faith Fallout" folder identification name was thus immediately apparent, satisfying the second requirement of the plain view doctrine.

¶30 However, the third requirement, that the officers have lawful access to the object, is not met in this case. This requirement has been understood to preclude officers from seizing an item that is in plain view but is in an area that cannot be lawfully reached—for example, when officers can see stolen cars but would have to commit a warrantless trespass across the defendant's property to reach them. Horton, 496 U.S. at 137.

¶31 In executing a search warrant, police officers may search areas in which the items identified in the warrant might reasonably be found, including closed containers. People in Interest of D.F.L., 931 P.2d 448, 452 (Colo. 1997); see also People v. Koehn, 178 P.3d 536, 537 (Colo. 2008) (where warrant authorized search of defendant's residence for firearms and ammunition, officers were justified in searching kitchen cabinet and pants and seizing incriminating items found there in plain view). We analogize the "Faith Fallout" text message folder to a closed container, which Detective Slattery opened to discover its contents—namely, the text messages between Faith W. and Herrera. Here, the warrant authorized Detective Slattery to search for messages between "Stazi" and Herrera. The question, then, is whether the "Faith Fallout" folder was a container in which messages from "Stazi" could reasonably be found. We agree with the trial court that it was not.

¶32 The trial court concluded that in searching Herrera's cell phone, Detective Slattery was authorized to search for messages from "Stazi's," or Detective Dodd's, number. As noted above, however, the police had an objective basis to believe that the "Faith Fallout" folder was associated with a different number—that is, one that belonged to Faith W., not Detective Dodd. Furthermore, there was no evidence before the trial court that a specific folder in the Kik application could contain messages from multiple numbers. Instead, the evidence indicated that each folder could only be associated with a single number. And the trial court specifically found that there was no link between the "Stazi" number and the "Faith Fallout" folder. Thus, because the evidence objectively indicated that the "Faith Fallout" folder contained messages from Faith W. and only Faith W., the police had no objective basis to conclude that the folder would contain messages from "Stazi."

¶33 In other contexts, courts have recognized that defendants can easily conceal the identity of contraband by mislabeling a container. See United States v. Riley, 906 F.2d 841, 845 (2d Cir. 1990) ("[F]ew people keep documents of their criminal transactions in a folder marked 'drug records.'"). In the computer file context, in fact, the Fourth Circuit has noted that a search of computer files "c[an] not be limited to reviewing only the files' designation or labeling, because the designation or labeling of files on a computer can easily be manipulated to hide their substance." United States v. Williams, 592 F.3d 511, 522 (4th Cir. 2010); see also United States v. Burgess, 576 F.3d 1078, 1093 (10th Cir. 2009) (upholding a warrant against a particularity challenge, and noting that the

warrant could not be limited to certain computer file names where "illegal activity may . . . well be coded or otherwise disguised").

¶34 Here, however, the People did not present a shred of evidence to suggest, nor did they attempt to argue, that Herrera had "manipulated" the Kik files "to hide their substance." Williams, 592 F.3d at 522; see also United States v. Richards, 659 F.3d 527, 536, 541–42 (6th Cir. 2011) (upholding search of all the files on a computer where the investigator specifically testified that, in his experience, suspects frequently mislabeled files). On the contrary, their evidence indicated that the "Faith Fallout" file corresponded with the name of Herrera's suspected victim, Faith W., and thus it was reasonable for them to believe that the messages in that folder were from the actual victim, not Detective Dodd. In other words, the circumstances suggested that the files had not been deceptively labeled. As such, because there was no evidence that Herrera might have mislabeled the folders, the mere, abstract possibility that he could have done so did not give Detective Slattery reason to believe that the "Faith Fallout" folder contained messages from "Stazi." We therefore conclude that the trial court was correct in determining that messages from Detective Dodd could not be reasonably found in that folder. Any search of the "Faith Fallout" folder would require an additional warrant. See, e.g., United States v. Corral, 970 F.2d 719, 725 (10th Cir. 1992) (in some circumstances, the plain view doctrine "may support the warrantless seizure of a container believed to contain contraband[,] but any subsequent search of the concealed contents of the container must be accompanied by a warrant or justified by one of the exceptions to the warrant requirement") (emphasis in original).

¶35 If we were to hold that any text message folder could be searched because of the abstract possibility that it might have been deceptively labeled, we would again be faced with a limitless search, as with the People's first argument. We instead proceed cautiously in applying the plain view doctrine to searches involving digital data. Cf. People v. Gall, 30 P.3d 145, 154 (Colo. 2001) (noting privacy concerns with a search that follows the lawful seizure of a computer "container" that could reasonably contain writings identified in a search warrant). Where such a search does not meet the traditional requirements of Fourth Amendment doctrine, it should not be permitted. For example, in Riley, the Court held that police could not search a suspect's cell phone as part of a search incident to arrest as a general matter because the traditional justifications for a search incident to arrest were not met; as the Court concluded, cell phone data does not present danger to arresting officers and is not usually susceptible to immediate destruction. 134 S. Ct. at 2485–88. Most importantly, the Court recognized that "[m]odern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'" Id. at 2494–95 (citation omitted). That is the case here. Because Detective Slattery did not have lawful access to the "Faith Fallout" folder, the third requirement of the plain view exception is not met. The plain view exception therefore does not apply.

III.

¶36 Because the text messages between Herrera and Faith W. do not fall within the warrant issued in this case or within the plain view exception to the warrant

requirement, they were properly suppressed by the trial court. We therefore affirm the court's suppression order.

CHIEF JUSTICE RICE dissents, and **JUSTICE BOATRIGHT** joins in the dissent.

CHIEF JUSTICE RICE, dissenting.

¶37 I disagree with the majority's application of the plain view doctrine to the "Faith Fallout" folder. Because I believe that the Faith Fallout text message folder was within the scope of the warrant, I would hold that the content of that folder—the text message conversation between Faith W. and Herrera—satisfies the plain view warrant exception and thus should not be suppressed. In my view, the warrant authorizing the search of Herrera's cell phone for text messages sent between Herrera and Stazi necessarily authorized a search of all text conversations on Herrera's phone because Herrera easily could have disguised the conversation under an alternate name.

¶38 Whether Herrera actually hid text messages in the Faith Fallout folder is irrelevant. Evidence—or a lack of evidence—before the trial court suggesting that Herrera did not actually alter the file names has no bearing on whether it was reasonable for an officer to suspect that messages could be hidden in that folder. Because the Faith Fallout folder contained text messages, it was objectively reasonable to search the folder for text messages between Herrera and Stazi. Once the searching officer lawfully opened the folder, the texts themselves between Herrera and Stazi satisfied the plain view exception to the warrant requirement.

¶39 In sum, because the warrant itself authorized the officer to search the Faith Fallout folder for texts between Herrera and Stazi, and because the messages that he discovered within that folder between Faith W. and Herrera satisfy the plain view exception to the warrant requirement, I would reverse the trial court's suppression order regarding the contents of the Faith Fallout folder. I therefore respectfully dissent.

I. The Scope of the Warrant

¶40 The Fourth Amendment of the United States Constitution protects "against unreasonable searches and seizures" and requires that warrants issue only "upon probable cause . . . and particularly describing the place to be searched, and the persons or things to be seized." This search "is not limited by the possibility that separate acts of entry or opening may be required to complete the search." United States v. Ross, 456 U.S. 798, 821 (1982). When a searching officer executes a valid warrant, he "may search closed containers [found within the authorized space] so long as the containers are of the type within which the items . . . might reasonably be found." People in Interest of D.F.L., 931 P.2d 448, 452 (Colo. 1997).

¶41 To meet this requirement, the container must be (1) "large enough to contain the contraband or evidence" that is the subject of the warrant and (2) a place where that evidence "might reasonably [have been] expected to be secreted." Id. (alteration in original) (quoting United States v. Evans, 92 F.3d 540, 543 (7th Cir. 1996)). This reasonableness requirement does not depend on the subjective perceptions of the searching officer, nor does it depend on subsequent proof that the officers' expectations were correct. Rather, reasonableness "is measured in objective terms by examining the totality of the circumstances." People v. Mendoza-Balderama, 981 P.2d 150, 157 (Colo. 1999) (quoting Ohio v. Robinette, 519 U.S. 33, 39 (1996)). Moreover, although officers must operate generally within the bounds of the warrant, "when [the warrant's] limits have been precisely defined, nice distinctions between . . . containers . . . must give way

to the interest in the prompt and efficient completion of the task at hand." Ross, 456 U.S. at 821. In the context of electronics, "[i]t is unrealistic to expect a warrant to prospectively restrict the scope of a search by directory, filename or extension." United States v. Burgess, 576 F.3d 1078, 1093 (10th Cir. 2009).

¶42 In this case, Detective Dodd sought and obtained a warrant to search Herrera's seized cell phone for the following: (1) texts sent between Herrera and Stazi, (2) photographs sent between Herrera and Stazi that were attached to text messages, and (3) indicia of ownership to show the phone belonged to Herrera. Because Herrera's phone was not compatible with the police department's digital search tool, the officer had to search the phone's text messages manually and take pictures of relevant evidence. Given the malleability of digital data and the real potential that Herrera disguised these texts under another name or folder, however, it is unreasonable to restrict such manual searches to folders labeled "Stazi."[1] Rather, as the above caselaw indicates, a warrant allowing an officer to search a digital device for text messages

[1] Indeed, as the Tenth Circuit observed in United States v. Burgess, "a computer search may be as extensive as reasonably required to locate the items described in the warrant." 576 F.3d 1078, 1093 (10th Cir. 2009) (quoting United States v. Grimmet, 439 F.3d 1263, 1270 (10th Cir. 2006)). Thus, the court observed:

> It is unrealistic to expect a warrant to prospectively restrict the scope of a search by directory, filename or extension to attempt to structure search methods—this process must remain dynamic. While file or directory names may sometimes alert one to the contents . . . illegal activity may not be advertised even in the privacy of one's personal computer—it could well be coded or otherwise disguised.

Id. As any smartphone user is surely aware, a recipient of text messages or communications from another number may label that number however he pleases, and so the folder name under which texts are cataloged deserves little weight, if any.

between two parties should be interpreted as authorizing the officer to search every text message folder because any of those folders could reasonably contain the evidence detailed in the warrant.

¶43 Because the Faith Fallout folder potentially could have been mislabeled to cover up Herrera's illegal communications with Stazi, it was objectively reasonable for the officer to open that folder, pursuant to the warrant, to search for those communications. Therefore, opening the Faith Fallout folder did not implicate the plain view doctrine at all; it was simply an authorized search pursuant to the warrant. The plain view doctrine only came into play once the officer had opened the Faith Fallout folder and observed the incriminating text messages between Herrera and Faith W. therein.

II. The Plain View Doctrine

¶44 In order to be admissible, evidence discovered pursuant to a search either must be obtained via a valid search warrant or must meet an exception to the warrant requirement. People v. Gothard, 185 P.3d 180, 183 (Colo. 2008). The exception at issue here, the plain view doctrine, "allows police to seize, without a warrant, evidence that is plainly visible, so long as: (1) the initial intrusion onto the premises was legitimate; (2) the police had a reasonable belief that the evidence seized was incriminating; and (3) the police had a lawful right of access to the object." Id.

¶45 Although this test was originally conceived in the context of physical, tangible space, it translates easily to the digital space of a smartphone. Here, the cell phone is the premises, the Faith Fallout folder is the object, and the contents of the Faith Fallout

folder—the messages between Herrera and Faith W.—are the evidence seized. The first element is easily satisfied. The warrant authorized searching the phone for messages between Herrera and Stazi, so the initial intrusion into the phone was legitimate under the warrant. See id. at 183. The second element is satisfied because the incriminating nature of the texts between Herrera and Faith W. would have been immediately apparent to the searching officer. See id. at 184. The officer knew that Herrera allegedly had been inappropriately communicating with Faith W., a juvenile; Faith Fallout was almost certainly a pseudonym that shared the first name of the juvenile with whom Herrera allegedly had been communicating; and the inculpatory nature of the text messages would have been immediately apparent. See id. at 183–84.

¶46 Finally, the police had a lawful right of access to the Faith Fallout folder because it could have concealed the Stazi text messages, which were the subject of the warrant, thereby satisfying element three of the plain view doctrine. See id. A reasonable officer could conclude that a folder containing text messages could contain the text messages between Herrera and Stazi. File names are easily manipulated, so it is objectively reasonable to think that text messages within the scope of the warrant could be found in the Faith Fallout folder. The folder was, therefore, a closed container "of the type within which the items named in the warrant might reasonably be expected to be secreted." See People in Interest of D.F.L., 931 P.2d at 452. Whether Herrera actually hid messages from Stazi in the Faith Fallout folder is irrelevant. It only matters that it was objectively reasonable for an officer to search the folder for text messages between Herrera and Stazi.

¶47 Therefore, although the text messages within the Faith Fallout folder were themselves beyond the scope of the warrant, their seizure satisfied all three elements of the plain view doctrine. The texts fell within an exception to the warrant requirement and should not have been suppressed.

III. Conclusion

¶48 In the end, my disagreement with the majority turns on whether the Faith Fallout folder was within the scope of the warrant authorizing a search of Herrera's phone for text messages between Herrera and Stazi. I would hold that it was. The officer lawfully accessed both the phone and the Faith Fallout folder under the warrant, and the incriminating nature of the texts contained within that folder would have been immediately apparent to him in light of his previous knowledge. I would hold that the texts are admissible under the plain view doctrine. Therefore, I respectfully dissent.

I am authorized to state that JUSTICE BOATRIGHT joins in this dissent.