



DenverDA

Mitchell R. Morrissey, District Attorney - Second Judicial District
201 W. Colfax Avenue, Dept. 801, Denver, CO 80202

Bus. Phone: 720-913-9000
Fax: 720-913-9035

MEMORANDUM

TO: Judge Gilman; Abe Hutt
FROM: Robin Whitley
SUBJECT: Thoughts on a recommendation for changes to Criminal Rule 41 to address electronic storage media and electronically stored information
DATE: 4/12/2017

Subcommittee colleagues:

I throw this out, as a starting point for our considering a recommendation to the committee for amendment of Rule 41. The aim is to have the rule address search warrants regarding electronic storage media and electronically stored information. First is language we could consider for our rule and accompanying comments. Next are the corresponding excerpts from the federal rule reflecting language adopted in 2009; with these excerpts are the related advisory committee notes.

I believe that the clarity and modernization this change would deliver would be of benefit to the bench, forensic examiners, and detectives. It would greatly help to get the language and concepts more in line with current technological and forensic realities.

After our committee's last meeting, the court of appeals addressed one of the central questions this proposal involves: the applicability *vel non* of the 14-day warrant-execution deadline to the post-seizure examination of the storage media. *People v. Reahal*, 2017 COA 18, ¶¶ 27-31. I attach a copy of that opinion.

I also attach a copy of *People v. Gall*, 30 P.3d 145 (Colo. 2001). This opinion does not deal specifically with the issues involved in the rule-change proposal. But it might be helpful background reading—particularly its acknowledgment of the frequent need to conduct examinations later, off-site, as well as its discussion that reveals the broad view of “documents,” “writings,” and the like in the computer context that necessarily has evolved and that is implicated in the proposal. See *Gall*, 30 P.3d at 153-55.

4/12/2017

Page 2

Proposed rule change: Amend Crim. P. 41(d)(5)(VI) and add 41(d)(5)(VII), and add comments, as follows:

(VI) A search warrant shall be executed within 14 days after its date. The officer taking property under the warrant shall give to the person from whom or from whose premises the property was taken a copy of the warrant and a receipt for the property or shall leave the copy and receipt at the place from which the property was taken. The return shall be made promptly and shall be accompanied by a written inventory of any property taken. The inventory shall be made in the presence of the applicant for the warrant and the person from whose possession or premises the property was taken, if they are present, or in the presence of at least one credible person other than the applicant for the warrant or the person from whose possession or premises the property was taken, and shall be verified by the officer. In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied. The judge upon request shall deliver a copy of the inventory to the person from whom or from whose premises the property was taken and to the applicant for the warrant.

(VII) A warrant under Rule 41(b) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(d)(5)(VI) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

Comments

2017

Subdivision (d)(5)(VII). Computers and other electronic storage media commonly contain such large amounts of information that it is often impractical for law enforcement to review all of the information during execution of the warrant at the search location. This rule acknowledges the need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant.

4/12/2017

Page 3

The term “electronically stored information” is intended to be sufficiently broad and flexible to cover all current types of computer-based information and to encompass future changes and developments.

The amended rule does not address the specificity of description that the Fourth Amendment and Colorado Constitution Article II, Section 7, may require in a warrant for electronically stored information, leaving the application of this and other constitutional standards concerning both the seizure and the search to ongoing case law development.

References:

Fed. R. Crim. P. 41(e)(2)

(B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

ADVISORY COMMITTEE NOTES

2009 Amendments

Subdivision (e)(2). Computers and other electronic storage media commonly contain such large amounts of information that it is often impractical for law enforcement to review all of the information during execution of the warrant at the search location. This rule acknowledges the need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant.

The term “electronically stored information” is drawn from Rule 34(a) of the Federal Rules of Civil Procedure, which states that it includes “writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can

4/12/2017

Page 4

be obtained.” The 2006 Committee Note to Rule 34(a) explains that the description is intended to cover all current types of computer-based information and to encompass future changes and developments. The same broad and flexible description is intended under Rule 41.

In addition to addressing the two-step process inherent in searches for electronically stored information, the Rule limits the 10 [14]1 day execution period to the actual execution of the warrant and the on-site activity. While consideration was given to a presumptive national or uniform time period within which any subsequent off-site copying or review of the media or electronically stored information would take place, the practical reality is that there is no basis for a “one size fits all” presumptive period. A substantial amount of time can be involved in the forensic imaging and review of information. This is due to the sheer size of the storage capacity of media, difficulties created by encryption and booby traps, and the workload of the computer labs. The rule does not prevent a judge from imposing a deadline for the return of the storage media or access to the electronically stored information at the time the warrant is issued. However, to arbitrarily set a presumptive time period for the return could result in frequent petitions to the court for additional time.

It was not the intent of the amendment to leave the property owner without an expectation of the timing for return of the property, excluding contraband or instrumentalities of crime, or a remedy. Current Rule 41(g) already provides a process for the “person aggrieved” to seek an order from the court for a return of the property, including storage media or electronically stored information, under reasonable circumstances.

Where the “person aggrieved” requires access to the storage media or the electronically stored information earlier than anticipated by law enforcement or ordered by the court, the court on a case by case basis can fashion an appropriate remedy, taking into account the time needed to image and search the data and any prejudice to the aggrieved party.

4/12/2017

Page 5

The amended rule does not address the specificity of description that the Fourth Amendment may require in a warrant for electronically stored information, leaving the application of this and other constitutional standards concerning both the seizure and the search to ongoing case law development.

Fed. R. Crim. P. 41(f)(1)

(B) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. The officer must do so in the presence of another officer and the person from whom, or from whose premises, the property was taken. If either one is not present, the officer must prepare and verify the inventory in the presence of at least one other credible person. *In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied.* The officer may retain a copy of the electronically stored information that was seized or copied.

ADVISORY COMMITTEE NOTES

2009 Amendments

Subdivision (f)(1). Current Rule 41(f)(1) does not address the question of whether the inventory should include a description of the electronically stored information contained in the media seized. Where it is impractical to record a description of the electronically stored information at the scene, the inventory may list the physical storage media seized. Recording a description of the electronically stored information at the scene is likely to be the exception, and not the rule, given the large amounts of information contained on electronic storage media and the impracticality for law enforcement to image and review all of the information during the execution of the warrant. This is consistent with practice in the “paper world.” In circumstances where filing cabinets of documents are seized, routine practice is to list the storage devices, i.e., the cabinets, on the inventory, as opposed to making a document by document list of the contents.

2017 WL 710478

NOTICE: THIS OPINION HAS NOT BEEN RELEASED FOR PUBLICATION IN THE PERMANENT LAW REPORTS. A PETITION FOR REHEARING IN THE COURT OF APPEALS OR A PETITION FOR CERTIORARI IN THE SUPREME COURT MAY BE PENDING.

Colorado Court of Appeals,
Div. VII.

The PEOPLE of the State of Colorado, Plaintiff-Appellee,
v.
Bradford Steven RAEHAL,
Defendant-Appellant.

Court of Appeals No. 15CA0414
|
Announced February 23, 2017

Synopsis

Background: Defendant was convicted in the District Court, Weld County, Shannon D. Lyons and Todd L. Taylor, JJ., of sexual assault on a child by one in a position of trust, sexual assault on a child as part of a pattern of abuse, and sexual exploitation of a child for the possession and production of sexually exploitative material, was adjudicated a habitual sex offender against children, and was designated as a sexually violent predator. Defendant appealed.

Holdings: The Court of Appeals, Harris, J., held that:

[1] trial court was not required to separately analyze photographs depicting abuse of first victim to determine whether sexual conduct shown in photographs was sufficiently similar to sexual conduct described by second victim;

[2] photographs depicting abuse of first victim were not unduly inflammatory, and thus were not unduly prejudicial under rule providing for exclusion of evidence if its probative value was substantially outweighed by danger of unfair prejudice;

[3] any error in trial court's failure to give instruction limiting purposes for which jury could consider defendant's conduct against first victim in determining guilt as to second victim did not constitute plain error;

[4] digital camera seized from defendant's residence was within scope of search warrant;

[5] second search warrant was not required for police to conduct forensic analysis of digital camera; and

[6] trial court did not err by admitting evidence that defendant had committed three prior acts of sexual assault on children, under statute permitting admission of such evidence and rule permitting admission of evidence of other acts; but

[7] trial court did not make any specific findings of fact before designating defendant as sexually violent predator, as required by statute governing such designations, and

thus designation would be vacated and case remanded.

Affirmed in part, vacated in part, and remanded.

Weld County District Court Nos. 12CR424 & 12CR506, Honorable Shannon D. Lyons, Judge, Honorable Todd L. Taylor, Judge

Attorneys and Law Firms

Cynthia H. Coffman, Attorney General, Patricia R. Van Horn, Senior Assistant Attorney General, Denver, Colorado, for Plaintiff-Appellee

Krista A. Schelhaas, Alternate Defense Counsel, Littleton, Colorado, for Defendant-Appellant

Opinion

Opinion by JUDGE HARRIS

*1 ¶ 1 Bradford Steven Raehal was convicted of multiple sexual offenses in connection with his sexual abuse of two boys, S.F. and J.H. On appeal, he argues that the district court erred in granting the prosecution's joinder motion, denying his motion to suppress evidence, and admitting unproven prior acts evidence under CRE 404(b).

¶ 2 We reject each of these contentions, and therefore affirm Raehal's convictions. However, Raehal also contends that the court erroneously designated him a sexually violent predator without making the

necessary findings. We agree, and thus we vacate this designation and remand for appropriate findings.

I. Background

¶ 3 Raehal was living in the basement of S.F.'s family home when he was arrested for failing to register as a sex offender. Shortly after the arrest, S.F. disclosed that Raehal had sexually assaulted him on numerous occasions.

¶ 4 During a forensic interview, S.F. detailed the assaults and reported that Raehal had taken nude pictures of him on a digital camera. Police officers thereafter obtained and executed a search warrant for Raehal's residence and seized the digital camera. Forensic analysis of the camera recovered thirteen previously deleted pictures of S.F. and Raehal engaged in sexual activity.

¶ 5 J.H., who also lived at S.F.'s house, initially denied that he was sexually assaulted by Raehal, but he later reported three separate incidents of sexual abuse. While the boys each reported different types of sexual contact, both S.F. and J.H. alleged that abuse occurred in Raehal's semitrailer, that Raehal had provided them with videogames, and that he initiated the contact by rubbing lotion on their backs.

¶ 6 Raehal was initially charged in separate cases for the incidents with S.F. (12CR424) and the incidents with J.H. (12CR506). The prosecution moved to join the cases before

trial, and the district court granted the motion over defense counsel's objection.

¶ 7 After a jury trial, Raehal was convicted of two counts of sexual assault on a child by one in a position of trust (one for acts against S.F. and one for acts against J.H.) and two counts of sexual assault on a child as part of a pattern of abuse (one for acts against S.F. and one for acts against J.H.). He was further convicted of two counts of sexual exploitation of a child for the possession and production of sexually exploitative material relating to the pictures taken of S.F. In a separate proceeding, Raehal was adjudicated a habitual sex offender against children. The district court designated him a sexually violent predator and sentenced him to 112.5 years to life in the custody of the Department of Corrections.

II. Joinder

¶ 8 Raehal contends that the district court erred in joining the cases alleging abuse of S.F. and J.H. While he admits that S.F.'s testimony would have been admissible as CRE 404(b) evidence in the case relating to J.H., he insists that the cases were improperly joined because the explicit photographs depicting Raehal and S.F. engaged in sexual acts would not have been admissible in J.H.'s trial.

*2 ¶ 9 Although Raehal objected to the pretrial joinder of the cases, the People contend that Raehal waived this claim because he did not renew his objection during trial. See *People v. Bondsteel*, 2015

COA 165, ¶ 27, —P.3d —— (*cert. granted Oct. 31, 2016*). We disagree, and conclude that the claim was adequately preserved.

¶ 10 The division in *Bondsteel* held that an objection to joinder is unpreserved if not renewed at trial, *id.*, but the division also acknowledged that its holding departed from nearly fifteen years of contrary precedent. See *People v. Gross*, 39 P.3d 1279, 1282 (Colo. App. 2001) (requiring only a pretrial objection to preserve the issue). Raehal's trial preceded the *Bondsteel* decision. Accordingly, we decline to impose its new rule on Raehal. See *Bondsteel*, ¶ 30 (recognizing that, “[t]o hold that the issue is waived, despite this precedent, could be a retroactive application of a new rule, which might implicate due process”).

¶ 11 A trial court may order two or more criminal complaints to be tried together if the offenses could have been joined in a single complaint. Crim. P. 13. Two or more offenses may be charged in the same charging document if the offenses are of the same or similar character or are based on two or more connected acts or transactions or parts of a larger scheme or plan of action. Crim. P. 8(a)(2).

[1] [2] ¶ 12 We review a decision concerning the joinder of separate charges for an abuse of discretion. *People v. Curtis*, 2014 COA 100, ¶ 14, 350 P.3d 949. An abuse of discretion occurs when the joinder causes actual prejudice as result of the jury's inability to separate the facts and legal theories applicable to each offense. *Id.* at ¶ 15; *People v. Gregg*, 298 P.3d 983, 985-86

(Colo. App. 2011). There is no prejudice where evidence of each offense would be admissible in separate trials. *Gregg*, 298 P.3d at 986.

¶ 13 Pursuant to CRE 404(b), evidence of other crimes, wrongs, or acts is inadmissible if its relevance depends on an inference that the person has a bad character and acted in conformity with that character. However, this evidence may be admissible for other purposes. CRE 404(b); *see also* § 16-10-301(1), C.R.S. 2016 (permitting the prosecution to introduce evidence of other sexual offenses for any purpose other than propensity because “such evidence of other sexual acts is typically relevant and highly probative”).

[3] ¶ 14 Raehal concedes that, under CRE 404(b), S.F.’s testimony describing the sexual assaults would have been admissible in a separate trial on the charges related to J.H., but he insists that the photographs depicting the abuse would not have been admissible. According to Raehal, the court should have conducted a separate Rule 404(b) analysis with respect to the photographs and determined that the sexual conduct shown in the photographs was not sufficiently similar to the sexual conduct described by J.H. For example, Raehal says, S.F. and J.H. both testified that Raehal rubbed lotion on them as a prelude to sexual activity, but the photos did not depict that particular conduct.

¶ 15 We disagree that the district court was required to separately analyze the photos under CRE 404(b). Raehal does not allege that the taking of the photographs was

an independent prior bad act under Rule 404(b). The photographs were admitted not to prove a common scheme or plan but simply to corroborate S.F.’s testimony. *See People v. Roark*, 643 P.2d 756, 762 (Colo. 1982) (“[P]hotographs are admissible to depict graphically anything a witness may describe in words.”); *see also People v. Herrera*, 2012 COA 13, ¶ 33, 272 P.3d 1158. When photographs are admitted for this purpose, the admissibility test articulated in *People v. Spoto*, 795 P.2d 1314, 1318 (Colo. 1990), is inapplicable.

*3 [4] [5] [6] [7] ¶ 16 Accordingly, we need only address Raehal’s claim that the photographs were unduly prejudicial under CRE 403. Pursuant to Rule 403, “evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice.” CRE 403. Photographs are not inadmissible “merely because they present vividly to the jurors the details of a shocking crime.” *People v. Villalobos*, 159 P.3d 624, 630 (Colo. App. 2006) (quoting *Martinez v. People*, 124 Colo. 170, 177, 235 P.2d 810, 814 (1951)). Nor are they rendered inadmissible because these “grim details ... might shock or otherwise upset the trier of fact.” *People v. Drake*, 748 P.2d 1237, 1248 (Colo. 1988). Evidence is only unfairly prejudicial if it has an undue tendency to suggest a decision on an improper basis such as sympathy, hatred, contempt, retribution, or horror. *People v. Rath*, 44 P.3d 1033, 1043 (Colo. 2002). While the photographs are undoubtedly upsetting, given their probative value in corroborating S.F.’s testimony and proving the sexual assault, we cannot say that they are unduly inflammatory in the

context of a sexual assault on a child case. *See People v. Dunlap*, 975 P.2d 723, 747 (Colo. 1999) (Photos of entry wounds “were not particularly shocking in the context of a murder.”); *People v. Guffie*, 749 P.2d 976, 983 (Colo. App. 1987) (probative value outweighed prejudice of graphic pictures of homicide victim, even though witness had already testified to the contents of the photos).

[8] [9] ¶ 17 Raehal also contends that the district court further erred by failing to provide an instruction limiting the purposes for which the jury could consider his conduct against S.F. in determining guilt as to J.H. *See* § 16-10-301(4)(d). However, because defense counsel did not request such an instruction when the evidence was introduced, we analyze this issue under the plain error standard of review. *People v. Underwood*, 53 P.3d 765, 771 (Colo. App. 2002). Under plain error, we will reverse only if the error was obvious and “undermined the fundamental fairness of the trial itself so as to cast serious doubt on the reliability of the judgment of conviction.” *People v. Miller*, 113 P.3d 743, 750 (Colo. 2005) (quoting *People v. Sepulveda* 65 P.3d 1002, 1006 (Colo. 2003)).

¶ 18 Even if we assume the court erred by failing to give a limiting instruction, any error did not affect the reliability of the judgment of conviction.

¶ 19 Although it did not provide a limiting instruction directing the jury not to consider any evidence of other acts as propensity evidence, the district court

specifically instructed the jury that “[e]ach count charges a separate and distinct offense and the evidence and law applicable to each count should be considered separately, uninfluenced by your decision as to any other count.” We presume the jury followed this instruction, which similarly limited the jury’s consideration of the evidence. *See Curtis*, ¶ 23.

¶ 20 In sum, because any error could not have cast serious doubt on the reliability of the judgment of conviction, reversal is not required.

III. Seizure and Subsequent Search of Digital Camera

¶ 21 Raehal further contends that the district court erred in denying his motion to suppress the explicit photographs because the digital camera on which they were discovered was outside the scope of the search warrant. In the alternative, he asserts that even if the camera was properly seized, it was illegally searched because it was not analyzed until months later, long after the warrant had expired. We reject both contentions and conclude that the district court did not err in denying Raehal’s motion to suppress.

[10] [11] ¶ 22 Appellate review of a ruling on a motion to suppress presents a mixed issue of fact and law. *People v. Pitts*, 13 P.3d 1218, 1221-22 (Colo. 2000). While we will defer to a trial court’s findings of fact that are supported in the record, the trial court’s legal conclusions are subject to de novo review. *Id.* at 1222.

¶ 23 The search warrant specifically authorized the seizure of “any and all computer systems and computer equipment,” “any and all storage media,” and “any and all computer peripheral devices attached or unattached to the computer to include but not limited to ... physical devices which serve to transmit or receive information to and from the computer.” The warrant also authorized the officers to look for and seize “images, video, or drawings which portray child pornography.” In addition, the warrant affidavit reported S.F.’s statement that the defendant had taken digital pictures of him with a gray or silver digital camera.

*4 [12] ¶ 24 In deciding whether items discovered during the execution of a search warrant are within the scope of the warrant, police officers are not obliged to interpret its terms narrowly. *People v. Gall*, 30 P.3d 145, 153 (Colo. 2001).

[13] ¶ 25 We agree with the district court that digital cameras “are certainly physical devices that can transmit and receive information from computers,” and, therefore, the digital camera seized from Raehal’s residence was within the scope of the search warrant.

[14] ¶ 26 Moreover, when executing a warrant, officers may search the location, including any containers or “technological containers” at that location that are reasonably likely to contain items described in the warrant. *Id.* (upholding seizure of computer because it was reasonably likely to

serve as a “container” for writings). Here, the officers were authorized to search for images of child pornography, and the digital camera was reasonably likely to serve as a “technological container” for these images, especially in light of the victim’s statement, contained in the affidavit, that Raehal had taken pictures of him with a digital camera. Accordingly, the camera was properly seized pursuant to the warrant.

[15] ¶ 27 Raehal asserts, in the alternative, that even if the camera was lawfully seized, it was unlawfully searched because the forensic analysis occurred outside the statutory fourteen-day time frame for executing the warrant. See § 16-3-305(6), C.R.S. 2016; Crim. P. 41(d). According to his argument, because the original warrant had expired before the camera was searched, unless the police obtained a second warrant, the later analysis of the camera constituted an unconstitutional warrantless search.

[16] ¶ 28 The warrant, though, was executed within the fourteen-day deadline. The requirement that search warrants be executed promptly prevents officers from conducting searches long after the probable cause supporting the search has expired. See *People v. Russom*, 107 P.3d 986, 991 (Colo. App. 2004); see also *United States v. Brewer*, 588 F.3d 1165, 1173 (8th Cir. 2009). But in this case, when the warrant was executed, the officers still had probable cause to believe that the camera would be found in Raehal’s house and that it would contain images of child pornography.

[17] ¶ 29 The officers were not required to conduct an analysis of the digital camera at Raehal's house. Typically, search warrants which specifically authorize the seizure of technology contemplate the later search of that media. *See United States v. Gregoire*, 638 F.3d 962, 967-68 (8th Cir. 2011).¹

1 We note the Federal Rules of Criminal Procedure analog to Crim. P. 41(d) was amended in 2009 to state that, “[u]nless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.” Fed. R. Crim. P. 41(e)(2)(B).

[18] ¶ 30 And a second warrant to search properly seized media is not necessary where the evidence obtained in the search does not exceed the probable cause articulated in the original warrant. *See United States v. Evers*, 669 F.3d 645, 652 (6th Cir. 2012); *see also United States v. Grimmett*, 439 F.3d 1263, 1268-69 (10th Cir. 2006). Here, based on an affidavit establishing probable cause, the search warrant expressly authorized the examination of any computer and storage devices for images of child pornography. Because the images could not have been altered or deleted once the camera was seized, probable cause for the search did not dissipate in the interval between the initial seizure of the camera and its subsequent search. *Brewer*, 588 F.3d at 1173 (Because the evidence at issue was “electronically-stored files in the custody of law enforcement[,] ... the several months’ delay in searching the media did not alter the probable cause analysis.”); *United States v. Burgess*, 576 F.3d 1078, 1097 (10th Cir. 2009) (“Probable cause to search was unaffected

by the delay and the reasons to search the computer and hard drives did not dissipate during the month and a half the items sat in an evidence locker.”); *United States v. Syphers*, 426 F.3d 461, 469 (1st Cir. 2005) (One-year delay in searching computer after it was seized did not invalidate the search because the delay did not “cause[] a lapse in probable cause.”).

*5 [19] ¶ 31 The cases Raehal cites do not undercut this rule. In those cases, a second warrant to search electronic media was required because, while conducting the subsequent search of the media, evidence of a different crime was inadvertently uncovered. Generally, to continue to search for evidence of this second crime, a second search warrant is required. *See United States v. Carey*, 172 F.3d 1268, 1270 (10th Cir. 1999) (the original warrant authorized a search of the computer for evidence related to illegal drug sales; when the officers found evidence of another crime—possession of child pornography—another warrant was needed to search for this evidence); *Grimmett*, 439 F.3d at 1268 (“[L]aw enforcement may not expand the scope of a search beyond its original justification.”). Where, as here, the evidence uncovered on the media was within the scope of the original search warrant, the original warrant is sufficient to authorize the search. *See Grimmett*, 439 F.3d at 1268 (distinguishing *Carey* and concluding that the original warrant authorized the subsequent computer search because the evidence uncovered was within the original justification for the search and seizure of the computer).

IV. Factual Predicate for CRE 404(b) Evidence

[20] ¶ 32 At trial, pursuant to Rule 404(b), the prosecution presented evidence of two previous incidents in which Raehal had sexually assaulted minor boys. Raehal contends that this evidence was improperly admitted because the prosecution's offer of proof was inaccurate. We are not persuaded.

[21] ¶ 33 Before a trial court may admit other acts evidence, it must first determine whether the prosecution has established by a preponderance of the evidence that the other act occurred and the defendant committed it. § 16-10-301(4)(b); *People v. Gallegos*, 226 P.3d 1112, 1116 (Colo. App. 2009). This determination may be made based on an offer of proof. § 16-10-301(4)(c).

¶ 34 Prior to trial, the prosecution moved to admit evidence, pursuant to section 16-10-301 and Rule 404(b), that Raehal had previously sexually assaulted two young boys. In the offer of proof, the prosecution summarized the boys' statements to police, which alleged that Raehal had sexually assaulted them after inviting them to his home to play video games. The detective's reports were attached to the offer of proof.

¶ 35 Shortly after the boys' disclosures to the police, Raehal was charged with two counts of sexual assault on a child and one count of sexual assault on a child as part of a pattern of abuse. Raehal was convicted of one count of sexual assault on a child, and a mistrial was declared on the other two counts.²

2

While the pattern of abuse count was dismissed by the court, the second sexual assault on a child count was dismissed by the prosecution after the victim's mother stated that she did not want to put her child through another trial.

¶ 36 In the motion to admit the Rule 404(b) evidence, the prosecutor accurately stated that these acts "resulted in a conviction for Sexual Assault on a Child in Adams County case 95CR1806." However, less accurately, she also averred that "[t]he defendant has been convicted of the offenses set forth in the Offer of Proof."

¶ 37 Despite the imprecise nature of this second statement, the court was not under any illusions that Raehal was convicted of both counts of sexual assault on a child arising out of the offer of proof. Rather, the court explicitly acknowledged that Raehal was only convicted of one count arising from these allegations, but nonetheless determined that the offer of proof was sufficient to find, by a preponderance of the evidence, that all of the prior acts occurred. *See Kinney v. People*, 187 P.3d 548, 554 (Colo. 2008) ("Prior act evidence can be admitted even though the defendant was acquitted of the criminal charges arising out of the act."). Accordingly, the district court's determination that the prior acts occurred was not based on erroneous information. Because Raehal does not otherwise challenge the admission of this evidence, we perceive no error.

V. Designation as a Sexually Violent Predator

***6 [22]** ¶ 38 Finally, Raehal contends, and the People concede, that the district court erred by designating him a sexually violent predator without first making specific findings of fact on the record.

¶ 39 Section 18-3-414.5(2), C.R.S. 2016, requires district courts to make specific findings of fact regarding whether a defendant is a sexually violent predator. *See People v. Loyas*, 259 P.3d 505, 512 (Colo. App. 2010); *People v. Tuffo*, 209 P.3d 1226, 1231 (Colo. App. 2009). But here, the district court did not make any findings on the record on this issue. Accordingly, we must vacate Raehal's sexually violent predator designation and remand for further findings. *See Tuffo*, 209 P.3d at 1231-32.

VI. Conclusion

¶ 40 The judgment of conviction is affirmed. We vacate the district court's determination that Raehal is a sexually violent predator, and remand for further findings on this issue.

JUDGE LICHTENSTEIN and JUDGE RICHMAN concur.

All Citations

--- P.3d ----, 2017 WL 710478, 2017 COA 18

30 P.3d 145
Supreme Court of Colorado,
En Banc.

The PEOPLE of the State of
Colorado, Plaintiff/Appellant,
v.

Michael John GALL,
Defendant/Appellee.

No. 00SA101.

|
March 5, 2001.

Defendant, who was charged with felony theft by receiving and felony possession of explosives and incendiary devices and parts, moved to suppress items seized during warrant-based residential search. The District Court, Boulder County, Daniel Hale, J., granted motion. State brought interlocutory appeal. The Supreme Court, Coats, J., held that: (1) affidavit that was submitted to obtain residential search warrant was an affidavit in support of, and requesting issuance of, a warrant to search particular apartment number at specified address, though apartment number did not appear in body of affidavit and affidavit itself specifically requested only a warrant to search another address; (2) omission from affidavit of the source of information concerning that specific apartment did not render affidavit a “bare bones” affidavit so as to preclude reasonable reliance by officers executing search; and (3) five laptop computers in closet were within scope of warrant authorizing, in part, the seizure of writings, journals, and other information involving use of explosives.

Reversed and remanded.

Martinez, J., filed a dissenting opinion in which Hobbs and Bender, JJ., joined.

Attorneys and Law Firms

***146** Mary W. Keenan, District Attorney, Twentieth Judicial District, William F. Nagel, Chief Deputy District Attorney, Bryan W. Quiram, Deputy District Attorney, Boulder, CO, Attorneys for Plaintiff–Appellant.

***147** Paul Grant, Englewood, CO, Attorney for Defendant–Appellee.

Opinion

Justice COATS delivered the Opinion of the Court.

The People appealed pursuant to section 16–12–102(2), 6 C.R.S. (2000), and C.A.R. 4.1, challenging the district court's order suppressing all of the evidence seized during a search of the defendant's residence. Because the executing officers acted in reasonable reliance upon a search warrant and the seizure of five laptop computers, later determined to be stolen, was authorized by the warrant, the district court's order is reversed and the case is remanded for further proceedings consistent with this opinion.

I.

Following the seizure of numerous items, including suspected bomb-making materials; hundreds of **documents** referencing guns, explosives, and bomb making; writings about the defendant's personal feelings; and a number of desktop and laptop computers; the defendant was arrested and charged with one count of felony theft by receiving¹ and three counts of felony possession of explosives and incendiary devices and parts². The defendant moved to suppress everything seized from his residence on the ground that the supporting affidavit failed to articulate probable cause for the search. In addition, he challenged the seizure of five laptop computers, later determined to be stolen, on the ground that they were outside the scope of the warrant.³

1 § 18-4-410(1), 6 C.R.S. (2000).

2 § 18-12-109(6), 6 C.R.S. (2000).

3 On the day of the suppression hearing, the court granted the defendant's motion to sever the felony theft by receiving count from the three counts of felony possession of explosives and incendiary devices and parts.

At the February 7, 2000 hearing on the defendant's suppression motion, the People presented a copy of the warrant authorizing the search and the six-page, typewritten, supporting affidavit, as well as the testimony of Detective Hartkopp, who authored and presented the affidavit, and Detective Spraggs, who helped execute the search warrant. In the affidavit, Hartkopp outlined his investigation from June 24–26, 1999, into an alleged conspiracy between the defendant, Michael John Gall, and a co-worker, Byron Kyle Dorethy, to murder two

of their supervisors at Amgen Incorporated. Detective Hartkopp was assigned to the case following a report to the Boulder Police Department by several Amgen supervisors. An employee named Israel Ramirez had advised them that the defendant and Dorethy, both security guards at Amgen, had been talking about shooting fellow employees at work, including two of the security supervisors named David Barley and Debbie Payne. In subsequent interviews with the police, Ramirez gave details about the alleged co-conspirators' plans to use explosives during an attack at the Amgen facility and their specific threats to shoot Barley and Payne. Ramirez specifically told Detective Hartkopp that the defendant claimed to have used explosives in the past and to have in his possession an AK-47 high-powered rifle, an AR-15 rifle, and a Beretta handgun.

The affidavit also recounted conversations with another employee named Dan Brunson. Although Brunson was unsure of any specific plans to hurt anyone or damage property, he indicated that the defendant had talked about keeping a fully automatic AK-47, an AR-15, and a Beretta handgun at his residence; that once while criticizing someone else for improperly handling explosives, the defendant had explained to Brunson how to make a bomb; and that Dorethy was an emotionally unstable and disgruntled employee. In addition, the affidavit described the discovery by Amgen supervisors of a five-page computer printout in a paperwork box belonging to Dorethy. The final page of the printout was dated the evening of June 23, and contained

the address of David Barley, including detailed directions and time of travel from the Amgen building to Barley's residence. The full printout also contained multiple references to AR-15 and AK-47 rifles and other weapons; laudatory comments about the effects of the recent mass shooting at Columbine High School; characterization of the *148 author's own thoughts about killing as "unhealthy;" and use of the name "Mike" in reference to the person to whom his comments were directed. The defendant was the only person with the first name "Mike" known to the security supervisors to be working at the Amgen facility at the same time as Dorothy.

The affidavit also included a number of corroborating details learned by the police during their investigation. These included comments by co-workers about the anger of both the defendant and Dorothy at the impending replacement of the security guards at Amgen by another service; discovery that the work schedules of the defendant and Dorothy placed them as the only two guards in the security office on the shift immediately preceding the discovery of the computer printout; and learning from the FBI that the defendant did not have a permit allowing him to possess a fully automatic weapon. Finally, the affidavit listed a street address as the defendant's residence, learned through the telephone directory, and a second street address, which named officers had personally visited and observed.

Detective Spraggs testified that he participated in the execution of the warrant

for the defendant's residence. Although he did not recall seeing the affidavit prior to executing the warrant, he was aware that it authorized the seizure of writings, journals, and other information involving the use of explosives, reflecting the thoughts of the defendant, or otherwise referencing a plan to execute some type of "event" at Amgen.⁴ In addition to hundreds of written **documents** and other things seized during the execution of the warrant, the police also seized two desktop model computers and five laptop computers. Additional warrants were later obtained to search the hard drive memories of these computers for evidence of the suspected conspiracy.

- 4 The precise language of the warrant authorized the seizure of:
- Any and all firearms and ammunition;
 - Any and all explosives or incendiary devices, or parts, as defined under CRS 18-12-109;
 - Any and all written or printed material which provides instructions or examples concerning the production or use of any firearms, ammunition, and explosive or incendiary devices or parts;
 - Any and all written or printed material which shows an intent to do physical harm or physical damage against any person or building;
 - Any **documents** or materials that show the occupier or possessor of the premises and vehicle.

At the conclusion of the hearing, the court delayed its ruling to consider questions concerning the identification of the defendant's residence that had not previously been addressed by the parties. On February 11, it issued a written order concluding that the search warrant for the defendant's apartment was invalid and that the executing officers could not have relied on it in good faith because of the supporting affidavit's failure to identify the defendant's street address as an apartment complex or to

specify his apartment number. The district court therefore suppressed everything seized in the search.

On February 23, the People requested a rehearing, without objection, making clear their intent to appeal and asking that the court rule as well on the original grounds asserted in the defendant's motion to suppress, in order to avoid piecemeal litigation of the suppression issues. The court set the rehearing for April 4, almost two months later. While not opening the hearing for additional evidence, the court heard argument and completed its ruling on the defendant's motion to suppress. Specifically, it addressed the defendant's challenge to the seizure of the five laptop computers. In this subsequent ruling, the district court found that although the computers were lawfully viewed by the police, there was nothing in their immediate appearance giving the officers any reason to connect them with criminal behavior. The court indicated that it was unable to conclude that a computer is analogous to a writing, journal, notebook, letter, or any other type of **document**. It ruled that the People failed to prove that this was the basis for the seizure of the computers and that the computers were lawfully within the scope of the warrant.

[1] On April 14, the People filed their notice of interlocutory appeal in this court ***149** pursuant to C.A.R. 4.1.⁵

5 The defendant contends that this court lacks jurisdiction to hear this interlocutory appeal because the People failed to file their notice of appeal within 10 days of the district court's initial order of February 11. We have previously held that a trial court is not only

permitted but under certain circumstances has a duty to reconsider suppression orders, and if it does so, the prosecution may appeal its modified ruling within the time limitations of C.A.R. 4.1. *People v. Melton*, 910 P.2d 672, 675 n. 5 (Colo.1996); *People in the Interest of J.C.*, 844 P.2d 1185, 1188 (Colo.1993). It is even more clear that by accepting an invitation to complete an earlier ruling on a motion to suppress, a trial court demonstrates that the later, rather than the earlier, ruling constitutes its completed ruling on the motion, from which an appeal may be taken.

II.

After the suppression hearing, the district court determined from its own observations that the affidavit, as distinguished from the warrant presented along with it, did not indicate that the defendant's address was an apartment complex or specify the number of the defendant's apartment. After articulating grounds to believe that both the defendant and Dorothy were involved in the conspiracy, and that items connected to the crime would be found at their respective residences, the affidavit stated that officers determined from the telephone directory that the defendant, Michael John Gall, lived at 3161 Madison in Boulder. It then described a second residence in greater detail at 664 Tantra Drive, noting that it was actually visited by the police. However, each page of the affidavit also contained the annotation, "Search Warrant: 3161 Madison N302," and the warrant presented to the magistrate along with the affidavit identified the premises to be searched as 3161 Madison Avenue, Apt. N302. The warrant further described that address as a "four-story apartment building, constructed of brick with brown siding and beige trim," and indicated that apartment

“N302” was located on the “North/West side” of the building, with an east front entrance, and that it had a rust colored door with a window, beige trim, a brass door handle, and rust colored numbers “N302” on its right side. The warrant also specifically incorporated by reference the affidavit of Detective Hartkopp, and both the warrant and affidavit cross-referenced Attachment A, containing the list of items for which seizure was authorized by the warrant.

Rather than finding that the affidavit failed to establish probable cause to believe the defendant was committing a crime or that items connected to the crime would be discovered at his residence, the district court found that Hartkopp's affidavit failed to identify the specific apartment that was the defendant's residence and failed to request a warrant to search that apartment. The court ultimately concluded that the affidavit “was so lacking in indicia of probable cause as to render the executing officer's reliance entirely unreasonable.”

The Fourth Amendment to the United States Constitution protects individuals from unreasonable searches and seizures. U.S. Const. amend. IV.; *People v. Altman*, 960 P.2d 1164, 1167 (Colo.1998). Although search warrants are not required by the text of the Fourth Amendment, the jurisprudence of the Supreme Court has consistently expressed a strong preference for warrants issued by neutral magistrates. *United States v. Leon*, 468 U.S. 897, 914, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984); *United States v. Ventresca*, 380 U.S. 102, 106–07, 85 S.Ct. 741, 13 L.Ed.2d 684 (1965); 2

Wayne R. LaFave, *Search and Seizure: A Treatise on the Fourth Amendment* § 3.1(a) (3d ed. 1996 & Supp.2001). Even the text of the Fourth Amendment specifies, however, that warrants may issue only upon probable cause and must particularly describe the place to be searched and the person or things to be seized. U.S. Const. amend. IV.

[2] [3] [4] Probability, not certainty, is the touchstone of reasonableness under the Fourth Amendment, and probable cause involves probabilities similar to the factual and practical questions of everyday life upon which reasonable and prudent persons act. *People v. Grazier*, 992 P.2d 1149, 1153 (Colo.2000); *People v. MacCallum*, 925 P.2d 758, 762 (Colo.1996). Similarly, the information that can be relied upon to establish probable cause need not be admissible evidence, but relatively complex rules have developed concerning *150 the nature and sources of information that may be considered sufficiently reliable. *Ventresca*, 380 U.S. at 109, 85 S.Ct. 741. Furthermore, unlike probable cause to arrest, which merely entails sufficient grounds to believe that a crime was committed and that the suspect committed it, *MacCallum*, 925 P.2d at 762, probable cause for a search implicitly requires both sufficient grounds to connect the sought-after items to a crime⁶ and grounds to believe those items will be located in the place to be searched at the time of the search, *People v. Quintana*, 785 P.2d 934, 936 (Colo.1990).

6 The notion of sufficient connection with a crime was long ago expanded beyond contraband, fruits of a crime, and instrumentalities used to commit a crime,

to include even “mere evidence” of a crime. *Warden v. Hayden*, 387 U.S. 294, 301, 87 S.Ct. 1642, 18 L.Ed.2d 782 (1967); *People v. Torand*, 622 P.2d 562, 567 (Colo.1981).

[5] Although exceptions to the warrant requirement are recognized in narrowly defined circumstances, where executive branch officers present their grounds for a search to a judicial magistrate and rely on a judicial determination of probable cause rather than their own, the public policy encouraging warrants dictates that probable cause be reviewed with deference to the issuing magistrate. See *Illinois v. Gates*, 462 U.S. 213, 239, 103 S.Ct. 2317, 76 L.Ed.2d 527 (1983). The appropriate question for a court reviewing a search authorized by a warrant is therefore whether the issuing magistrate had a substantial basis for issuing the search warrant rather than whether the reviewing court would have found probable cause in the first instance. *Id.*; see also *Ventresca*, 380 U.S. at 109, 85 S.Ct. 741; *People v. Randolph*, 4 P.3d 477, 482 (Colo.2000); *Quintana*, 785 P.2d at 937.

[6] However, even where no substantial basis is found to support issuance of a search warrant, the exclusionary rule will not be applied if its purposes would be more costly than beneficial. *Leon*, 468 U.S. at 920–21, 104 S.Ct. 3405. The exclusionary rule is designed to deter police misconduct and to hold the executive branch accountable for official police misconduct. *Id.* at 916, 104 S.Ct. 3405; *Altman*, 960 P.2d at 1170; *People v. Deitchman*, 695 P.2d 1146, 1152 (Colo.1985)(Erickson, C.J., concurring). Because neutral judicial officers have no stake in the outcome of particular criminal proceedings, the threat of exclusion

cannot be expected to significantly modify their behavior. *Leon*, 468 U.S. at 916, 104 S.Ct. 3405; see also *Deitchman*, 695 P.2d at 1152 (Erickson, C.J., concurring); *id.* at 1160 (Dubofsky, J., concurring). Therefore, where a police officer relies in good faith on a facially valid warrant, the purpose of the exclusionary rule is not furthered by the suppression of relevant and probative evidence. *Leon*, 468 U.S. at 926, 104 S.Ct. 3405, *Deitchman*, 695 P.2d at 1160 (Dubofsky, J., concurring).

[7] [8] While it may be presumed that an officer was acting in good faith if he was acting pursuant to a warrant, see § 16–3–301(1), 6 C.R.S. (2000); *Randolph*, 4 P.3d at 483; *Altman*, 960 P.2d at 1169–70, see also *United States v. Cardall*, 773 F.2d 1128, 1133 (10th Cir.1985) (*Leon* good faith principle creates a presumption that when an officer relies upon a warrant, the officer is acting in good faith), exclusion is still called for whenever the officer “lacks reasonable grounds for believing that the warrant was properly issued.” *Leon*, 468 U.S. at 923, 104 S.Ct. 3405, *Altman*, 960 P.2d at 1169–70. In *Leon*, the Court specified four situations in which this would be the case. An officer lacks reasonable grounds where (1) the warrant was issued on the basis of a deliberately false affidavit; (2) the issuing magistrate or judge has wholly abandoned his or her neutral and detached role; (3) the warrant is so facially deficient that the executing officer cannot reasonably believe the warrant is valid; or (4) the affidavit is so lacking in indicia of probable cause that official belief in its existence is unreasonable. *Leon*, 468 U.S. at 923, 104

S.Ct. 3405. Where the warrant is not facially deficient and there is no suggestion of misbehavior by the police or magistrate, the exclusionary rule will therefore generally fail in its purposes unless it would be apparent to a reasonably well-trained officer that the affidavit was inadequate. *Id.* at 926, 104 S.Ct. 3405; *Altman*, 960 P.2d at 1169–70 (officer's good faith reliance *151 not to be impugned unless “entirely unreasonable” to believe the affidavit supported issuance of the warrant).

After the testimony and argument at the original suppression hearing, the district court observed what neither counsel had detected. In the body of the affidavit, the street address attributed to the defendant from the telephone directory did not include an apartment number. Moreover, the affidavit made a specific request for a warrant to search the Tantra Drive address, not the Madison Avenue address. Focusing on the distinction between the warrant and the affidavit, the district court concluded that the affidavit by itself failed to identify or request a warrant to search the defendant's apartment and that the information included in the warrant could not be considered to remedy that omission.

[9] The distinction between a search warrant and a supporting affidavit, however, is not so technical or inflexible. Each performs a separate function, but the Fourth Amendment does not mandate that certain information appear in a **document** entitled, “Warrant,” and other information appear in a **document** entitled, “Affidavit.” Here, both **documents** were prepared by the same

officer and presented to the magistrate at the same time. There can be no doubt that the affidavit, which contained on every page the annotation, “Search Warrant: 3161 Madison N302,” and which accompanied an unsigned warrant to search Apartment N302 of the four-story apartment complex at 3161 Madison Avenue in Boulder, was an affidavit in support (and requesting issuance) of the warrant to search that apartment. Under these circumstances, there was never any danger of confusion about the specific apartment for which the search was authorized. Similarly, when the warrant and annotation are considered along with the statement in the body of the affidavit identifying the defendant's address as 3161 Madison, there can be no doubt that the affiant effectively identified apartment N302 at 3161 Madison Avenue as the defendant's residence, one of the two residences for the search of which the affidavit provided probable cause.

[10] Regardless of the form of the **documents**, however, a search warrant must be supported by probable cause to search a specific place. *Randolph*, 4 P.3d at 481. This requires sufficient information to permit the issuing magistrate to evaluate the source and reliability of the affiant's information. *Gates*, 462 U.S. at 238, 103 S.Ct. 2317; *Randolph*, 4 P.3d at 484. While the information contained in the affidavit and warrant in this case adequately identified a specific apartment as the defendant's residence, it nevertheless failed to indicate the affiant's source of that information. With respect to this single link in the chain of inferences required for probable cause to search the particular

apartment that was searched, the affidavit was silent and therefore arguably failed to provide a substantial basis for the issuing magistrate's action.

Even under these circumstances, however, the exclusionary sanction should not have been applied unless the affidavit was so lacking in indicia of probable cause that official belief in its existence was unreasonable. *Leon*, 468 U.S. at 926, 104 S.Ct. 3405; *Altman*, 960 P.2d at 1169–70. Such an affidavit has been characterized as a “bare bones” affidavit, referring to its conclusory nature. *Randolph*, 4 P.3d at 482; *Altman*, 960 P.2d at 1170. Although a well-trained officer must be expected to know that a magistrate must be given sufficient information to enable the magistrate to evaluate the conclusions asserted by the affiant, a number of courts have found it easy to understand how an officer, and even an issuing magistrate, might overlook a lack of detail on a point that is so common or public that it can often be established by the telephone book or the name on a mailbox. See *United States v. Shutters*, 163 F.3d 331, 337–38 (6th Cir.1998) (where affidavit describes defendant's address with such particularity that the common sense inference is the affiant personally observed the residence, or determined through investigation defendant was associated with premises, the omission does not render the affidavit “bare bones”), cert. denied, 526 U.S. 1077, 119 S.Ct. 1480, 143 L.Ed.2d 563 (1999); *United States v. Procopio*, 88 F.3d 21, 28 (1st Cir.1996) (affidavit is not “bare bones” where only omission is affiant's *152 failure to express

how he knew given address was the defendant's, as it is “easy to understand how both the officer applying for the warrant and the magistrate might overlook a lack of detail on a point often established by the telephone book or the name on a mailbox”), cert. denied, 519 U.S. 1138, 117 S.Ct. 1008, 136 L.Ed.2d 886 (1997); see also *United States v. Shea*, 211 F.3d 658, 666 (1st Cir.) (while questioning whether expressly providing basis for knowledge of defendant's residence in affidavit is a required link in the chain, court ultimately concluded that even if it was a necessary link omission of this information was a minor, and not necessarily infrequent, error encompassed by the *Leon* good faith exception), cert. denied, 531 U.S. 1154, 121 S.Ct. 1101, 148 L.Ed.2d 973 (2001); *United States v. Brown*, 832 F.2d 991, 994–96 (7th Cir.1987) (officer's belief that warrant authorized search, even though containing only a conclusory statement linking defendant to premises to be searched, was objectively reasonable and good faith exception applied), cert. denied, 485 U.S. 908, 108 S.Ct. 1084, 99 L.Ed.2d 243 (1988); *State v. Varnado*, 675 So.2d 268, 270–71 (La.1996) (officer and magistrate's failure to notice omission of information linking the defendant to the searched residence was objectively reasonable and application of exclusionary rule could serve no remedial purpose); *Braxton v. State*, 123 Md.App. 599, 720 A.2d 27, 48 (1998) (where affidavit reasonably implied residence to be searched was the defendant's, and probable cause existed to search defendant's residence, good faith doctrine could fill any potential gap in the factual basis underlying the affiant's assertions).

In this case, the suspect was not unidentified, a fugitive from justice, or a transient without regular living quarters. He was a security guard, employed by the very company initiating the investigation, living at an apartment complex in the city, with an address listed in the telephone book. The affidavit recounted conversations with his co-workers and supervisors over a three-day investigation and gave a detailed description of the exterior of his apartment, clearly requiring someone's first-hand observations. Nothing in the six-page affidavit suggests any irregularity in the defendant's living arrangements or reason to suspect stealth or deception with regard to the location of his residence. Furthermore, neither the police nor the magistrate noticed the omission when the warrant was issued, and neither the attorneys nor the district court specifically identified a problem with the source of the apartment number, even at the suppression hearing or on appeal.

[11] Not every instance of insufficient attention to detail by police officers, any more than by attorneys or judges, is unreasonable. *See Deitchman*, 695 P.2d at 1158 (Dubofsky, J., concurring) (failure of affiant to include how he knew defendant's address was not so "egregious" as to render reliance on the warrant "entirely unreasonable"). If the good faith exception to the exclusionary rule applied only to matters as to which reasonable minds could differ, it would add nothing to the substantial basis standard of review that predated its development. At least where, as here, the affidavit merely fails to provide

support for an easily obtained and seemingly obvious piece of information, that omission does not render an otherwise detailed and complex affidavit a "bare bones" affidavit. In the absence of any evidence of a deliberately false affidavit, abandonment by the judge of his duty, or a facially deficient warrant, the exclusion of evidence discovered in reliance on the search warrant in this case was improper.

III.

For separate reasons the defendant challenged the seizure of five laptop computers, which were later determined to be stolen and provided the basis for a charge of felony theft by receiving. At the suppression hearing, Detective Spraggs testified that in addition to hundreds of writings and bomb-making materials, the police seized two desktop computers that had been assembled in the defendant's living room, five laptop computers found in individual carrying cases on the floor of one of the defendant's closets, a fax machine, and a projector. Spraggs also related his understanding that the warrant authorized the seizure of any written or printed items pertaining to guns, explosives, the *153 making of explosives, the defendant's personal thoughts, or plans to execute some type of "event" at Amgen. He further made clear his personal awareness, prior to executing the warrant, that the Internet could be used to obtain and download materials on bomb making and that people routinely use computers as word processors and for the exchange of e-mail.

Although the trial court did not initially rule on this challenge, it ultimately ruled that computers were not analogous to writings, and therefore seizure of the computers was outside the scope of the warrant. The court premised this ruling on its recollection that the People had not presented any evidence indicating that this was “the type of thing typically stored on a computer,” and that the People had not proven by a preponderance of the evidence that this was the purpose for seizing these computers.

[12] [13] In deciding whether items discovered during the execution of a search warrant are within the scope of the warrant, police officers are not obliged to interpret its terms narrowly. *United States v. Hill*, 19 F.3d 984, 987 (5th Cir.)(quoting *United States v. Stiver*, 9 F.3d 298, 302–03 (3d Cir.1993)), cert. denied, 513 U.S. 929, 115 S.Ct. 320, 130 L.Ed.2d 281 (1994); see also *United States v. Somers*, 950 F.2d 1279, 1285 (7th Cir.1991), cert. denied, 504 U.S. 917, 112 S.Ct. 1959, 118 L.Ed.2d 561 (1992); *United States v. Lucas*, 932 F.2d 1210, 1215–16 (8th Cir.), cert. denied, 502 U.S. 949, 112 S.Ct. 399, 116 L.Ed.2d 348 (1991). They may search the location authorized by the warrant, including any containers at that location that are reasonably likely to contain items described in the warrant. See *In re D.F.L.*, 931 P.2d 448, 451–52 (Colo.1997); *People v. Press*, 633 P.2d 489, 492–93 (Colo.App.1981) (upholding officer's removal and subsequent search of defendant's safe at another location where safe was reasonably believed to contain items sought pursuant to a valid

search warrant); see also *United States v. Gomez-Soto*, 723 F.2d 649, 654–55 (9th Cir.1984) (upholding seizure of briefcase where warrant authorized seizure of books, papers, diaries, and receipts), cert. denied, 466 U.S. 977, 104 S.Ct. 2360, 80 L.Ed.2d 831 (1984). This container rationale is equally applicable to nontraditional, technological “containers” that are reasonably likely to hold information in less tangible forms. See *United States v. Meriwether*, 917 F.2d 955, 958 (6th Cir.1990) (upholding search of “pager” where warrant authorized seizure of phone numbers); *Gomez-Soto*, 723 F.2d at 654–55 (upholding seizure of cassette tapes where warrant authorized seizure of books, papers, diaries, and receipts). Similarly a warrant cannot be expected to anticipate every form an item or repository of information may take, and therefore courts have affirmed the seizure of things that are similar to, or the “functional equivalent” of, items enumerated in a warrant, as well as containers in which they are reasonably likely to be found. See *Hill*, 19 F.3d at 987–89 (check stubs as functional equivalent of cash disbursement journals), cert. denied, 513 U.S. 929, 115 S.Ct. 320, 130 L.Ed.2d 281 (1994); *United States v. Word*, 806 F.2d 658, 661 (6th Cir.1986) (patient sign-in sheets, receptionist day sheets, encounter sheets and forms, and admission records deemed to be the functional equivalent of medical records, payment records, and appointment records), cert. denied, 480 U.S. 922, 107 S.Ct. 1383, 94 L.Ed.2d 697 (1987); *United States v. Reyes*, 798 F.2d 380, 383 (10th Cir.1986) (cassette tapes as functional equivalent of writings.); *United States v. Musson*, 650 F.Supp. 525, 531–32, 539 (D.Colo.1986)

(computer disks and diary as functional equivalent of various specified types of **documents**, writings, and records evidencing money laundering or narcotics trafficking); *see also* LaFave, *supra*, § 4.11(c), at 692.

[14] [15] Contrary to the holding of the trial court, the computers found in the defendant's closet were reasonably likely to serve as "containers" for writings, or the functional equivalent of "written or printed material," of a type enumerated in the warrant. The executing officers were authorized to seize materials that provided instructions or examples concerning the production or use of any firearms, ammunitions, and explosive or incendiary devices or parts, as well as materials showing an intent to do physical harm or physical damage against any person or building. *154 The computers were not found in a packaged state or in any way suggesting that they could not have been used for the purposes for which they were designed. The officers had already found an abundance of written materials in the defendant's residence that were described in the warrant, and the unchallenged testimony of Detective Spraggs made clear his conscious consideration of the computers' usefulness for correspondence and downloading information from the Internet. In any event, the subjective motive of an executing officer is inconsequential to the seizure of items pursuant to a search warrant. A policeman's ulterior motive could no more bar a search within the scope of a properly issued warrant than could his pure heart entitle him to exceed the scope of the warrant. *United States v. Ewain*, 88

F.3d 689, 694 (9th Cir.), *cert. denied*, 519 U.S. 944, 117 S.Ct. 332, 136 L.Ed.2d 244 (1996); *see also Whren v. United States*, 517 U.S. 806, 813, 116 S.Ct. 1769, 135 L.Ed.2d 89 (1996) (subjective intentions of police officers play no role in ordinary, probable-cause Fourth Amendment analysis); *Scott v. United States*, 436 U.S. 128, 137–38, 98 S.Ct. 1717, 56 L.Ed.2d 168 (1978) (officer's actions, and not his underlying intent or motivation, are determinative in a Fourth Amendment analysis.); *Altman*, 938 P.2d at 146.

[16] Rather than attempting to "search" the computers at the scene, the officers merely seized the computers and sought further search warrants to inspect their contents. For various policy reasons, the removal of a sealed container, which may amount to an "over-seizure," is not only authorized but preferred in limited circumstances, including where "the sorting out of the described items from the intermingled undescribed items would take so long that it is less intrusive merely to take that entire group of items to another location and do the sorting there." LaFave, *supra*, at § 4.11(a), p. 686; *see also United States v. Hargus*, 128 F.3d 1358, 1363 (10th Cir.1997) (seizure of filing cabinets for later search off-site reasonable where impractical to sift through all records on site), *cert. denied*, 523 U.S. 1079, 118 S.Ct. 1526, 140 L.Ed.2d 677 (1998); *United States v. Shilling*, 826 F.2d 1365, 1369–70 (4th Cir.1987) (seizure of filing cabinet for search at another location permissible where volume of **documents** in cabinets made on-site search for authorized **documents** impractical), *cert. denied*, 484

U.S., 1043, 108 S.Ct. 777, 98 L.Ed.2d 863 (1988); *United States v. Johnson*, 709 F.2d 515, 516 (8th Cir.1983) (permissible for officers to remove locked safe reasonably believed to contain items sought pursuant to valid warrant from the premises to another location where it could be opened); *United States v. Abrahams*, 493 F.Supp. 310, 313 (S.D.N.Y.1980) (reasonable for officers to remove locked safe and locked filing cabinet where these “containers” could likely hold items sought via search warrant and exigent circumstances justify removal for search at different location).

Courts in other jurisdictions have found this rationale for the seizure and removal of containers not only applicable but in fact compelling with regard to computers. In addition to the problems of volume and commingling, the sorting of technological **documents** may require a search to be performed at another location “because that action requires a degree of expertise beyond that of the executing officers,” LaFave, *supra*, § 4.11(a), 686, not only to find the **documents** but to avoid destruction or oversearching. See *United States v. Upham*, 168 F.3d 532, 535–36 (1st Cir.) (permissible for agents to seize computer, computer equipment, and disks where search on the premises could not readily be performed), *cert. denied*, 527 U.S. 1011, 119 S.Ct. 2353, 144 L.Ed.2d 249 (1999); *United States v. Schandl*, 947 F.2d 462 (11th Cir.) (holding that to force agents to conduct a thorough search of a large volume of written **documents** and computer discs on-site would actually amount to more intrusive search requiring

substantially longer amount of time), *cert. denied*, 504 U.S. 975, 112 S.Ct. 2946, 119 L.Ed.2d 569 (1992); *United States v. Scott-Emuakpor*, No. 1:99-CR-138, 2000 WL 288443 (W.D.Mich. Jan. 25, 2000) (seizure of computer permissible where warrant authorized seizure of “certain computer files” and officer could not perform the necessary search to locate these files on-site); *United States v. Hunter*, 13 F.Supp.2d 574, 583 (D.Vt.1998) (affirming the wholesale seizure *155 of computer and computer equipment on grounds that it often is simply impractical to search computers on site; recognizing that computers are extremely vulnerable to tampering, hiding, and destruction; and stating that “until technology and law enforcement expertise render on-site computer records searching both possible and practical, wholesale seizures, if adequately safeguarded, must occur”); *United States v. Sissler*, No. 1:90-CR-12, 1991 WL 239000 (W.D.Mich. Aug. 30, 1991) (concluding that computer functions as a container for written “records,” and holding it reasonable for officers to seize computer and discs for subsequent search to be performed at another location by computer expert).

In fact, the more substantial problem that may arise is properly limiting a search of the contents of a lawfully seized computer, which is not at issue here. See *In re Subpoena Duces Tecum*, 846 F.Supp. 11, 13–14 (S.D.N.Y.1994) (quashing subpoena as too broad and noting technical methods of narrowing search of computer data to balance privacy in irrelevant **documents** intertwined with relevant **documents** sought

by government); Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 Harv. J.L. & Tech. 75, 78, 87–89 (1994). Here, the officers merely seized and inventoried the computers for a subsequent search pursuant to a second, more detailed warrant. At least where the police were executing a search warrant authorizing the seizure of written materials typically composed, sent, received, or stored on a personal computer, and the executing officers had actually found written materials at the defendant's residence within the scope of the warrant, it was reasonably likely that apparently operable personal computers also found at that residence would contain similar materials or their functional equivalent. Seizure of the computers was therefore authorized by the warrant.

IV.

In sum, the issuing magistrate was presented with a specific request for a warrant to search 3161 Madison Avenue Apartment N302, and the warrant he signed specifically authorized a search of that apartment. Although the affidavit failed to include information from which the magistrate could independently evaluate the affiant's identification of apartment N302 as the defendant's residence, under the circumstances of this case that omission was understandable and not so egregious as to render official belief in the existence of probable cause unreasonable. Finally, in the circumstances present here, the five laptop computers discovered in the

defendant's closet were reasonably likely to contain items identified in the warrant, and their seizure was authorized by the warrant. Therefore, the order of the district court suppressing everything seized from the defendant's residence, including the five laptop computers, is reversed, and the case is remanded for further proceedings consistent with this opinion.

MARTINEZ, J., dissents, and HOBBS and BENDER, JJ., join in the dissent.

Justice MARTINEZ dissenting:

The majority holds that the search warrant issued in this case authorizing a no-knock search does not violate the Fourth Amendment. In reaching this result, the majority reasons that the absence of probable cause in the affidavit for a particular apartment is insignificant, perhaps because they believe the affidavit may be supplemented by information in the search warrant form submitted to the judge. After approving a no-knock search based on a deficient affidavit, the majority holds that powerful and complex computer equipment may be seized because it is included in the term "written or printed material" particularly described in the warrant.

In my view, the failure of the affidavit here to provide probable cause to search a specific apartment created the grave and unacceptable risk that uninvolved innocent persons, who live in the apartment building indicated in the affidavit, would be mistakenly subjected to a no-knock search.

In addition, even when the information in the search warrant form, which was presented to the judge for possible signature, is improperly considered together with the affidavit, there is no probable cause to believe that incriminating evidence *156 may be found in the particular apartment specified in the warrant. Finally, the seizure of computers as "written or printed material" violates privacy interests protected by the Fourth Amendment. Accordingly, there are three critical areas where I disagree with the reasoning of the majority opinion.

First, we have always required that a magistrate find probable cause to search a particular apartment within the four corners of the supporting affidavit before issuing a warrant. The affidavit in this case simply does not state probable cause to search a specific and identifiable apartment. This deficient affidavit cannot be supplemented with an apartment number and a description of the exterior of the apartment that inexplicably appears in the search warrant issued by the magistrate, as the majority appears to permit.

Second, the majority believes that reliance upon the deficient affidavit is not unreasonable and satisfies the good faith exception to the exclusionary rule, perhaps because they permit that affidavit to be supplemented by the information in the search warrant form that was submitted to the judge. However, even if the information in the search warrant is improperly considered together with the deficient affidavit, that combined information fails to provide probable cause to believe that

the particular apartment specified is the apartment of the defendant, where it was likely that incriminating evidence would be found.

Third, because computers are different from writings, both in degree and in kind, I believe that a warrant authorizing the seizure of computers should state so specifically. Both the seizure of a computer and the search of a computer's data are separate and serious intrusions of individual privacy. Therefore, a warrant permitting the seizure of computers must also include measures to direct the subsequent search of the computer's data in a manner designed to protect intermingled information that is not properly the subject of the search.

Because I do not agree with the majority in these critical areas, I respectfully dissent.

I.

The People appeal the trial court's ruling to suppress certain items found at the apartment home of Michael Gall, the defendant. In a no-knock search of the defendant's residence, numerous items, including **documents**, writings, various desktop computer components, and five laptop computers, were seized. Gall moved to suppress items removed from his residence, arguing that the supporting affidavit failed to articulate probable cause for the search and that the items seized were beyond the scope of the search warrant.

The majority has set forth the information in the affidavit in detail and I do not repeat it here. There is an abundance of information implicating Gall. In addition, Gall's residence is specifically implicated as a place where Gall kept firearms, including at least one that would have been illegal for him to possess. The only reference in the affidavit related to computers is to a five-page computer printout that contained the address of one of the supervisors, references to some of the weapons, and many very disturbing remarks. However, the affidavit states that investigators found this printout in "a paperwork box belonging to" Byron Dorothy, a co-worker of Gall's, and that the printout appeared to be directed at Gall rather than produced by him.

The affidavit contains a statement that the "[a]ffiant feels that sufficient probable cause has been presented to the court for the issuance of a search warrant for 664 Tantra Drive." The affidavit also contains a description of the Tantra Drive location given by the officer who visited the residence. No such statement or description is given about the apartment building where the search was ultimately conducted.

The only information in the body of the affidavit about Gall's apartment is a statement that the affiant had been advised by another officer that Gall resided at 3161 Madison, and that this information had been obtained from the telephone book. The body of the affidavit does not indicate that the Madison location is an apartment building, which apartment in the building was Gall's, or how such information was obtained.

*157 In the bottom margin of each page, in a smaller font than the body of the affidavit, the language "Search Warrant: 3161 Madison N302," appears without any explanation. We have before us no information regarding who put that information on the affidavit, when they may have done so, or where the information was obtained.

In the suppression hearing, the same judge who had earlier issued the warrant found that the affidavit was insufficient precisely because it did not include the description of the address as an apartment complex and the specific apartment number. This judge explained that "[b]ecause the affidavit does not link apartment N302 to the alleged crimes, an issuing judge could not make an independent determination that probable cause existed to search the property listed on the face of the warrant." The judge further explained that the affidavit was deficient because it failed to identify the particular apartment in such a way as to assure that "an officer executing the warrant could with reasonable effort ascertain and identify that apartment as the correct place to search." The judge also commented that "it was fortuitous that the correct apartment was searched."

In a subsequent hearing, the trial court addressed the seizure of the computers¹ found at Gall's residence. The trial court did so at the request of the People so that this subsequent issue could be addressed on appeal if the trial court's determination of no probable cause was reversed. At this hearing,

the trial court indicated that the computers were not mentioned as items to be seized by the search warrant, there was no nexus between the laptop computers and suspected criminal conduct, the computers were not subject to the warrant as writings, and there was no evidence presented to support the notion that the computers contained any information relevant to the crimes suspected in the search warrant. Accordingly, the trial court concluded that the computers must also be suppressed on the additional ground that there was no probable cause to associate the five laptops with any alleged criminal activity.

1 The oral ruling by the trial court on this issue specifically addressed the five laptop computers seized during the execution of the search warrant because the defendant did not move to suppress the desktop computer components in this case. Thus, only the five laptops seized are at issue here. However, the analysis of the issues involved applies equally to both laptop and desktop computers.

II.

As a threshold matter, I observe that there is no question that the affidavit shows that there is probable cause to believe that illegal firearms may be found in Gall's residence. However, the question before us is different: whether the affidavit shows probable cause to support the search warrant issued for apartment N302 at 3161 Madison. Accordingly, I begin my analysis with a discussion of the established principle that probable cause for the specific place to be searched must be established within the four corners of the affidavit. To determine whether the affidavit demonstrates probable

cause, I do not initially analyze the information contained in the unsigned and unsworn search warrant form presented to the judge. Thus, I conclude that the affidavit fails to establish probable cause to search the specific apartment authorized in the warrant. However, I next consider the information in the unsigned warrant together with the affidavit because I believe that the majority may have improperly relied on the unsigned warrant. I conclude that even with the information in the warrant, probable cause is still not established to search that specific apartment, N302.

A.

A search warrant may only be issued upon a showing of probable cause, "supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV; *see also* Colo. Const. art. II, § 7. When a reviewing court examines a search warrant after the fact to determine if it was valid, that court must assess whether the affidavit provided a "substantial basis" for the conclusion that probable cause existed. *Illinois v. *158 Gates*, 462 U.S. 213, 239, 103 S.Ct. 2317, 76 L.Ed.2d 527 (1983); *see also People v. Randolph*, 4 P.3d 477, 481 (Colo.2000). The United States Supreme Court requires that probable cause for a search warrant must be established by information in the affidavit. *See United States v. Karo*, 468 U.S. 705, 719, 104 S.Ct. 3296, 82 L.Ed.2d 530 (1984) ("[I]f sufficient untainted evidence was presented in the warrant affidavit to

establish probable cause, the warrant was nevertheless valid.”); *Stone v. Powell*, 428 U.S. 465, 474, 96 S.Ct. 3037, 49 L.Ed.2d 1067 (1976)(rejecting petitioner's contention that police should be permitted to supplement information contained in an affidavit for a search warrant). We have consistently interpreted this requirement to mean that, in determining probable cause, a magistrate is limited to the information contained within the four corners of the affidavit. *See Randolph*, 4 P.3d at 481; *People v. Meraz*, 961 P.2d 481, 483 (Colo.1998). This does not mean that courts should read affidavits in a hypertechnical manner, but rather, they should use logic to determine whether or not probable cause is established. *See United States v. Ventresca*, 380 U.S. 102, 109, 85 S.Ct. 741, 13 L.Ed.2d 684 (1965).

Fourth Amendment analysis leads to the clear conclusion that an unsigned search warrant, presented to a judge for signature, may not be used to establish probable cause, but instead may only issue “on [an] affidavit sworn to or affirmed before the judge.” § 16–3–302, 6 C.R.S. (2000). Allowing search warrant forms, which are not signed or sworn by the affiant, to support inadequate affidavits creates a broad exception for deficient affidavits contrary to the requirements in the Colorado Constitution that “no warrant ... shall issue ... without probable cause, supported by oath or affirmation reduced to writing.” Colo. Const. art. II, § 7. The unsigned warrant in this case was not attached to, or incorporated by reference in, the affidavit, and thus is not verified by the affiant. *See People v. Campbell*, 678 P.2d 1035, 1040

(Colo.App.1983)(**documents** attached to and incorporated by reference in an affidavit fall within the four corners of the affidavit). Simply put, the information that appears in the warrant form cannot be relied upon because the source of the information is completely unknown.

The four corners of the affidavit must supply probable cause to believe that incriminating evidence could be found in a particular place. To do so here, the affidavit must establish a basis for believing that 3161 Madison Avenue N302 is Gall's home. Although the affidavit provides enough information to cause a neutral magistrate to reasonably believe that illegal firearms could be found at Gall's residence, it does not provide the kind of specific and detailed information that would allow the magistrate to determine where Gall's residence was located. While the affidavit states that the affiant personally spoke with another officer who had discovered that Gall lived at 3161 Madison in Boulder, it does not specify an apartment number or even indicate that the address given is an apartment building. The only detail that potentially evidences the apartment number is the inclusion of “Search Warrant: 3161 Madison N302” in the bottom margin on each page of the affidavit. There is no other information provided that suggests a specific apartment should be searched.

Apartment dwellers are entitled to the same constitutional protections against unlawful searches and seizures as persons living in single family homes. *People v. Arnold*, 181 Colo. 432, 434, 509 P.2d 1248, 1249

(1973); *see also People v. Avery*, 173 Colo. 315, 319, 478 P.2d 310, 312 (1970). The affidavit examined in *Arnold* related that an informant told police officers that the defendants were in possession of illicit drugs, that the informant had observed specific drugs at 2018 Ogden, and that the defendants lived in two particular apartments: the manager's apartment, and apartment No. 3 at 2018 Ogden. *Arnold*, 181 Colo. at 434, 509 P.2d at 1249. In *Arnold*, we suppressed the evidence seized in the searches, holding that although the affidavit related that the informant observed marijuana and "speed" somewhere in the building at 2018 Ogden, the affidavit failed to give any specific indication as to where in that multiple-occupancy structure the drugs were located. Thus, the affidavit failed to relate sufficient facts from which the issuing magistrate could find probable *159 cause to believe that the drugs were located within each of the defendant's apartments. *Id.* at 435, 509 P.2d at 1250. An affidavit that merely provides probable cause to search an apartment in an apartment house will not suffice as support for a warrant to search a particular unit. *See* 2 Wayne R. LaFave, *Search and Seizure: A Treatise on the Fourth Amendment* § 3.7(d), at 386 (3d ed. 1996 & Supp.2001).

In this case, the affidavit did not identify 3161 Madison as an apartment building, and it also failed to specifically state which apartment was Gall's. The inclusion of "Search Warrant: 3161 Madison N302" in the margin of the affidavit is of no assistance. There is nothing in the affidavit explaining who put this information in the margin

or when it may have been put there. This marginal information does not appear in the body of the affidavit and can hardly be regarded as verified by the affiant. Moreover, this apartment number in the margin is not associated in any way with Gall. Thus, because the four corners of the affidavit did not reveal that 3161 Madison is an apartment building, nor that N302 is a specific apartment within that building, a neutral magistrate could not have had sufficient facts to establish probable cause to issue a search warrant for that particular apartment. Accordingly, I must conclude that the affidavit fails to establish probable cause to support the search warrant issued for apartment N302.

B.

The majority appears to rely upon the unsigned search warrant to determine that probable cause existed to search apartment N302. However, even when we improperly consider the information in the unsigned warrant, that information, together with the information in the affidavit, does not demonstrate probable cause to search apartment N302. The warrant viewed in conjunction with the affidavit does not provide any basis to believe that Gall's apartment is number N302. The warrant merely describes the apartment building and the exterior of apartment N302. It does not associate Gall with that specific apartment. In addition, the source of information in the warrant is not revealed. The unsigned warrant and affidavit cannot establish probable cause to search apartment

N302 without any information connecting Gall to apartment N302.

The majority concludes that, despite the deficient affidavit, the exclusion of evidence discovered in reliance on the search warrant in this case was improper. In reaching this conclusion, the majority apparently relies upon the unsigned search warrant together with the affidavit, and looks to the good faith exception as detailed in *United States v. Leon*, 468 U.S. 897, 104 S.Ct. 3405 (1984). Claiming minor error, the majority holds that the warrant was not so deficient, nor was there any suggestion of misbehavior by the police or magistrate, such that the exclusionary rule should have been invoked. Thus, the majority holds that under the good faith exception to the exclusionary rule, the search performed pursuant to the warrant here was constitutional.

Under the good faith doctrine, the exclusionary sanction should not be applied unless an affidavit is so lacking in indicia of probable cause that official belief in its existence is unreasonable. *Leon*, 468 U.S. at 926, 104 S.Ct. 3405. I do not believe this case falls under the good faith exception to the exclusionary rule. For the reasons outlined above, I believe that the affidavit lacked any indicia of probable cause to the extent that official belief in its existence was unreasonable. In my view, even when improperly relying upon information in the unsigned search warrant, it is unreasonable to believe that probable cause existed. Thus, the good faith exception does not allow the unreasonable search and seizure here. While the application of the exclusionary

rule may lead to the undesirable result of losing evidence that may tend to show guilt in a serious and disturbing case, I believe we are bound to apply the law and affirm the trial court's suppression of the evidence.

III.

After deciding that the search of apartment N302 was constitutional, the majority holds that the language in the warrant authorizing the search of "written or printed material" is sufficiently particular to include computers.

*160 The majority's conclusion is based on its determination that a computer is essentially a storage device for writings. Thus, the majority allows the seizure of computers when search warrants only authorize the seizure of writings.²

2 The complete language in the search warrant is:

Any and all written or printed material which provides instructions or examples concerning the production or use of any firearms, ammunition, and [e]xplosive or [i]ncendiary devices or parts. Any and all written or printed material which shows an intent to do physical harm or physical damage against any person or building. Any **documents** or materials that show the occupier or possessor of the premises and vehicle.

In my view, the warrant here was insufficient to justify the seizure or search of the computers in this case because the warrant sought writings, not computers. Computers are far more complex and versatile than mere writings and their purpose is significantly different from just a container storing writings. As such, the warrant authorizing the seizure of writings was not sufficiently particularized to include computers. We require a warrant to particularly describe the

things to be seized in order to avoid the harm to privacy inherent in the seizure of items that are not the subject of a search. This purpose is not served if computers are seized when writings are sought. Finally, when the objects to be seized are intermingled with other objects that are not the subject of a search, special measures are required to protect the unrelated material. Therefore, I believe that the search and seizure of a computer must be specifically authorized in the search warrant and that such a warrant must include measures to direct the subsequent search of a computer's data.

A.

A search warrant must describe with particularity the place to be searched and the persons or things to be seized. U.S. Const. amend. IV; Colo. Const. art. II, § 7. The purpose of the particularity requirement is to prevent general searches. *People v. Staton*, 924 P.2d 127, 131 (Colo.1996)(citing *Maryland v. Garrison*, 480 U.S. 79, 84, 107 S.Ct. 1013, 94 L.Ed.2d 72 (1987)). Another purpose is to prevent the seizure of one thing under a warrant describing another. *People v. Hart*, 718 P.2d 538, 540 (Colo.1986). In order to comply with the Fourth Amendment, a search warrant must specify the items to be seized with sufficient particularity, so that nothing is left to the discretion of the officer executing the warrant. *People v. Lindholm*, 197 Colo. 270, 274, 591 P.2d 1032, 1035 (1979).

The question of whether evidence seized is within the scope of the warrant ultimately

turns on the *substance* of the items seized, not the label attached to the item. *United States v. Hill*, 19 F.3d 984, 988 (5th Cir.1994)(emphasis added). The Fifth Circuit in *Hill* considered whether check stubs were properly seized under a warrant seeking cash disbursement journals, and found that both items served the same purpose, because they both maintained a running account balance and traced the disposition of cash out of that account. *Id.* Thus, the Fifth Circuit concluded that the check stubs were the functional equivalent of the cash disbursement journals, and were therefore properly seized under the warrant.³

3 One judge dissented, arguing that check stubs are not the functional equivalent of cash disbursement journals, and that the interpretation that they were, improperly expanded the scope of the search warrant in violation of the particularity requirement. *Id.* at 991–92 (Politz, C.J., dissenting).

In determining whether a warrant is too general, or has properly met the particularity requirement, the nature of the property to be seized must be considered. *Lindholm*, 197 Colo. at 275, 591 P.2d at 1035. Here, the nature of the property seized under this warrant is particularly important, since computers, by their unique nature, raise special privacy concerns. Because computers process personal information and effects, they require heightened protection under the Fourth Amendment against unreasonable searches or seizures. Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 Harv. J.L. & Tech. 75, 80–83 (1994). “[C]omputers also raise particularity concerns because of their versatility.” *161 *United States v. Hunter*,

13 F.Supp.2d 574, 583 (D.Vt.1998). The Tenth Circuit has recognized that the storage capacity of computers requires a special approach to searches of computer files. *See United States v. Carey*, 172 F.3d 1268, 1273–77 (10th Cir.1999)(police exceeded scope of search warrant for computer files related to drug transactions when officer found child pornography files and continued search without obtaining additional search warrant). In order to explain why the nature of computers requires such a specialized approach, I generally discuss computers and then consider how they differ from writings and containers of writings.

B.

In this discussion, I describe some of the many functions and uses of a computer. I also explain that a computer stores or accesses data, and utilizes programs to process and present that data in a useable fashion.

Probably the most common function of a computer is its use as a word processor. Generally speaking, word processing programs assemble data that, when printed, may be considered a **document** of one form or another. When a user intentionally saves such a **document**, the computer stores information that it can gather and process to reproduce the **document**. Thus, in this limited sense, a computer is similar to a container, in that it has the capacity to reproduce writings from information that it has stored.

However, other aspects of word processing programs are very different from just a container in which writings are intentionally stored. For example, word processing programs also generally provide for retention of deleted **documents**. Most word processing programs use some form of a recycle bin, into which **documents** are transferred when deleted. Thus, a computer is also like a wastebasket of discarded material. In order to attempt to permanently delete such **documents**, the recycle bin must be emptied. However, even emptying the recycle bin may not actually delete the **document** or file because the information may still remain on the computer's hard drive.

The intentional deletion of a file does not permanently erase the file. *See Andrew Johnson-Laird, Smoking Guns and Spinning Disks*, 11 No. 8 Computer Law. 1, *5 (Aug.1994). Instead, the computer internally marks the file as not needed, and clears space for storage of other files. *Id.* The erasure of information only occurs when the computer overwrites the file with another file. *Id.* Even then, fragments of information may be retrievable if the entire file is not overwritten. *Id.* at *5–6. Furthermore, word processing programs may have saved portions or versions of **documents** regardless of whether the user intentionally saves the final version.

Thus, in general, a file or **document** may not be removed from the hard drive of a computer until it is reformatted. However, even then, it may be possible to partially recover **documents** or files removed from

a hard drive, depending on how the drive was reformatted. Further, the potential for deleted material to be stored on a hard drive, with or without intentional saving by the user, is not limited to word processing **documents**, but applies to other programs and functions of a computer as well. *See United States v. Upham*, 168 F.3d 532, 537 (1st Cir.1999)(discussing government's use of specialized utility program to search previously deleted images on computer); *United States v. Scott-Emuakpor*, No. 1:99-CR-138, 2000 WL 288443, at *3, 2000 U.S. Dist. LEXIS 3118, at *6 (W.D.Mich.2000)(noting that computer analyst was able to restore previously deleted files from computer during search of its contents pursuant to search warrant); *Commonwealth v. Copenhefer*, 526 Pa. 555, 587 A.2d 1353, 1354-57 (1991)(warrant authorizing seizure of computer sufficient to search contents, including deleted materials on hard drive).

A computer may also function as a transmitter of electronic mail, or e-mail. E-mail transmissions, which combine aspects of correspondence and recorded phone conversations, present special privacy issues. *See David J. Loundy, E-Law4: Computer Information Systems Law and System Operator Liability*, 21 Seattle Univ. L.R. 1075, 1079-80 (1998)[hereinafter *E-Law4*]. In addition to e- *162 mail capabilities, most computers in use today have internet access. Internet use raises complex issues due to the magnitude of information available, and the ability to download such information onto a computer, as well as the

storage within the computer's memory of the sites a user visited on the internet.

Computers serve these various functions by using programs to access databases and assemble information in a useful presentation. A database is a horizontally structured and vertically integrated collection of information or data. *See Seth Safier, Between Big Brother and the Bottom Line: Privacy in Cyberspace*, 5 Va. J.L. & Tech. 6, ¶ 51 (2000). Programs are also collections of information, but the information is organized as instructions to the computer. Programs and databases are the information that computers store, although computers may access other computers for programs or for databases. *See id.* at ¶ 50-58. Databases contain a vast array of information that is not organized in a particularly useful manner. Programs are used to organize, sort, process, modify, and display information in various useful presentations. *See id.*; *see generally State Court Adm'r v. Background Info. Servs.*, 994 P.2d 420 (Colo.1999)(discussing complexities of state-wide database of court records and potential privacy issues raised with releasing bulk data, even when protected information is deleted from database). If **documents** are actually produced from a database, they may differ, both in form and in the nature of information they contain, from any **document** a user may have intentionally stored.

Computers may also be part of a network, which is essentially an extension of the data contained in each individual computer

system. A network is a series of computers, usually linked via telephone or data wires, most often used to access resources from another computer. *See E-Law4, supra*, at 1077–79. Networked computers may also share programs. Networks expand the range of a computer's use, to include sending e-mail, direct communications between machines, transferring or sharing files, and downloading files. *Id.* at 1077–80. Moreover, any computer could be a server for other computers on a network.

Finally, the physical appearance of a computer, or its central processing unit (CPU), does not reveal the manner in which it is used. For example, the majority indicates that two desktop computers, along with five laptop computers, were seized during the execution of the search warrant here. However, the record suggests that a desktop computer with two CPU's was seized during the execution of the search warrant. The outward appearance of various components does not reveal how they were employed. In this way, a computer is unlike a physical container, where the types of objects held inside may be apparent. Instead, a computer's outward appearance provides no information regarding the extent of what may be stored inside or otherwise accessible through the computer.

Having generally discussed the complex nature of computers and commented on their multitude of functions and uses, I next consider how computers differ from mere writings and containers.

C.

A writing is limited in nature to something that has already been produced. A writing is “[t]he expression of ideas by letters visible to the eye. The giving of an outward and objective form to a contract, will, etc., by means of letters or marks placed upon paper, parchment, or other material substance.” Black's Law Dictionary 1609 (6th ed.1990). A computer is fundamentally different from a writing, or a container of writings, because of its capacity to hold a vast array of information in many different forms, to sort, process, and transfer information in a database, to provide a means for communication via e-mail, and to connect any given user to the internet. A computer may be comprised of a wide variety of personal information, including but not limited to word processing **documents**, financial records, business records, electronic mail, internet access paths, and previously deleted materials. Because of these differences, the seizure of a computer raises many issues beyond those that might pertain to mere writings.

***163** For example, seizing a computer may intrude into the privacy interests of individuals other than the intended subjects due to e-mail transmissions to and from a particular computer. Similarly, when a networked computer is subject to a search, it may be possible to examine interactions with computers that are networked to the one being searched. Moreover, the use of a computer to access the internet also

raises issues regarding a potential search of that computer, as the hard drive stores information about the internet sites that have been visited by the user. Therefore, the search of a computer could implicate the privacy concerns of many people who did not use a specific computer physically, but in fact used such computer electronically. Furthermore, the seizure of a networked computer may disrupt all or part of a network and interfere with many other users.

Aside from the clear differences between a writing and a computer, the analogy that the majority applies, considering computers as simply containers of writings, is not warranted by container law. As the majority notes, containers likely to hold items described in a search warrant may be seized and searched pursuant to a valid search warrant, so long as the containers are of the type within which the items named in the warrant might reasonably be found. *In re D.F.L.*, 931 P.2d 448, 452 (Colo.1997). Despite the complex nature of computers, the majority applies the container rule to computers, reasoning that the container rule has already been expanded to include items of an intangible nature, such as phone numbers on a pager, or a recording on a cassette tape.

The cases cited by the majority that apply container analysis to pagers and cassette tapes do not, in my opinion, provide support for the further expansion of container analysis to computers. See e.g., *United States v. Meriwether*, 917 F.2d 955, 958–60 (6th Cir.1990)(seizure of the defendant's telephone number from another person's

pager valid); *United States v. Gomez-Soto*, 723 F.2d 649, 655 (9th Cir.1984)(a microcassette is “by its very nature a device for recording information,” and was properly seized as a record); *United States v. Reyes*, 798 F.2d 380, 382–83 (10th Cir.1986)(cassette tape seized as record).

While these cases support the notion that pagers and cassette tapes may be analyzed under container law, it does not follow that this reasoning should apply to computers, since both a pager and a cassette tape are functionally different from a computer. Unlike a computer, both a pager and a cassette tape contain a finite amount of information of a limited type that is apparent from the nature of the device.

The majority also cites *United States v. Musson*, 650 F.Supp. 525 (D.Colo.1986), to support its view that a computer is the functional equivalent of a writing. In *Musson*, the seizure of computer diskettes, which occurred in 1982, was approved under a warrant authorizing the seizure of “any records or writings of whatsoever nature showing any business or financial transactions.” *Id.* at 531. Only computer diskettes were seized and searched in *Musson*, not entire computers. Moreover, computer diskettes produced in 1982, or earlier, were of very limited capacity and bear little resemblance to modern high-powered computers or even to modern computer disks. The rationale in *Musson*, which was based on the specific detail in the warrant, compared computer diskettes to cassette tapes. I do not find *Musson* useful

to a consideration of the issues raised by the full-scale seizure of a computer.

The majority also looks for support in a line of cases holding that seizure of containers believed to hold items sought in a search warrant may be removed from the premises in order to later search the contents. These cases have approved such seizures where searching the contents on the premises may be impractical due to the volume of materials seized, or the extensive time potentially required to search through the contents, or when a search of the contents at the site is impossible due to resistance of individuals present at a search. *See e.g., United States v. Hargus*, 128 F.3d 1358 (10th Cir.1997); *United States v. Shilling*, 826 F.2d 1365 (4th Cir.1987)⁴; *164 *United States v. Johnson*, 709 F.2d 515 (8th Cir.1983); *United States v. Abrahams*, 493 F.Supp. 310 (S.D.N.Y.1980). Generally, these cases do not dispense with the requirement that a warrant state the particular things to be seized. Rather, they concern the subsequent search of things described with particularity in the warrant, or clearly within the purview of the warrant, and properly seized.

4 In *Shilling*, the Fourth Circuit noted its reluctance to allow removal of file cabinets from the premises subject to a search warrant, stating “we cannot easily condone the wholesale removal of file cabinets and documents not covered by the warrant.” *Shilling*, 826 F.2d at 1369. Moreover, the Fourth Circuit noted its approval of the Ninth Circuit’s decision in *United States v. Tamura*, 694 F.2d 591 (9th Cir.1982), suggesting that when documents are so intermingled that sorting on site is not feasible, Fourth Amendment violations can be avoided by sealing the documents and obtaining an additional search warrant. *Shilling*, 826 F.2d at 1369. The Fourth Circuit concluded, however, that there were legitimate practical concerns

that prompted the removal of the file cabinets, and the seizure was not based on an intent to engage in a fishing expedition. *Id.* at 1369–70. Thus, the Fourth Circuit held that the documents had been lawfully seized. *Id.*

Nonetheless, the majority contends that this analysis has been extended to cases concerning the seizure of computers, citing to *Upham*, 168 F.3d 532, *United States v. Schandl*, 947 F.2d 462 (11th Cir.1991), *Scott–Emuakpor*, 2000 WL 288443, 2000 U.S. Dist. LEXIS 3118, *United States v. Hunter*, 13 F.Supp.2d 574 (D.Vt.1998), and *United States v. Sissler*, No. 1:90-CR-12, 1991 WL 239000, 1991 U.S. Dist. LEXIS 16465 (W.D.Mich.1991). With the exception of *Sissler*, these cases do not support the proposition that a seizure of computers for a later search off site is authorized by a search warrant that does not specifically include computers. Instead, these cases maintain that seizure of a computer may be required under some circumstances in order to facilitate the search of its contents when a warrant specifically authorizes the search and seizure of a computer. *See generally Upham*, 168 F.3d 532 (warrant authorizing search and seizure of computer software, hardware, disks, and drives sufficient to allow seizure of specified items, where search on premises of computer, including previously deleted materials, not feasible); *Schandl*, 947 F.2d 462 (warrant authorizing search and seizure of computer disks, memory storage devices, and mainframe sufficient for seizure of items specified, since search on premises would have been more disruptive than removing items from premises for more thorough, subsequent search); *Scott–Emuakpor*, 2000 WL 288443, 2000 U.S. Dist. LEXIS 3118

(under warrant seeking records, including all computer files, computer hard drives and disks were lawfully seized within the scope of the warrant, since police could not search for files without looking through hard drives and disks); *Hunter*, 13 F.Supp.2d 574 (warrant authorizing search and seizure of all computers, all computer storage devices, and all computer software systems, was not sufficiently particularized to allow seizure of computers, but good faith exception applied to save execution of the warrant because it was sufficiently limited to overcome the broad language of the warrant).

In contrast, *Sissler* does support the majority's view. See *Sissler*, 1991 WL 239000, 1991 U.S. Dist. LEXIS 16465. In *Sissler*, the district court concluded that computer disks and a computer were properly seized during the execution of a warrant looking for "records of drug transactions, records of assets purchased with the proceeds of marijuana transactions, and records identifying marijuana customers and suppliers." *Id.*, 1991 WL 239000 at *1, 1991 U.S. Dist. LEXIS 16465 at *7. The district court further justified the seizure under considerations of practicality. *Id.*, 1991 WL 239000 at *4, 1991 U.S. Dist. LEXIS 16465 at *12.

I would not follow *Sissler*. First, it is only one decision, authored by a district court judge in Michigan, with no precedential value. Second, the reasoning in *Sissler* is limited in that it simply states the proposition that it adopts, with little analysis. Finally, in my view, *Sissler* simply does not take into account the nature of computers.

Accordingly, because of the vast array of materials, the processing functions, and the immeasurable scope of information contained in computers, a computer is much, much more than merely a container of **documents** or writings. Therefore, the search warrant in this case authorizing the search and seizure of writings is not sufficiently particularized *165 to include computers. A "writing" is simply not particular enough to warrant a reasonable person to conclude that it includes a computer because a writing and a computer are two fundamentally different things, both in degree and in kind. It is unreasonable to conclude that a computer is the "functional equivalent" of a writing. The Fourth Amendment serves to protect citizens from unreasonable searches and seizures by the government. U.S. Const. amend. IV; Colo. Const. art. II, § 7. Moreover, Fourth Amendment analysis regarding the search and seizure of computers must be approached cautiously and narrowly because of the important privacy concerns inherent in the nature of computers, and because the technology in this area is rapidly growing and changing. Here, the seizure of the defendant's computers under the search warrant at issue was unreasonable.

D.

The majority suggests that the computers may be seized as writings, without taking into account the complexity of computers, because issues regarding the search of the computers' contents need not be addressed

in this case. Here, the police obtained a subsequent search warrant prior to actually searching the contents of the seized computers. However, under the majority's analysis, the computers may be seized as writings based on an interest in examining the content of those writings.⁵ The logical implication of the majority's approach is that the contents of a computer may be explored. Therefore, by analogizing a computer to a container of writings, the majority has taken a perilous step supporting an argument that a computer may be both seized and searched under a general warrant authorizing only the search and seizure of "writings."

5 I agree with the majority that the question of whether a seizure was proper is one of objective reasonableness, and is not based on the subjective intent of an officer executing a warrant. *Scott v. United States*, 436 U.S. 128, 138, 98 S.Ct. 1717, 56 L.Ed.2d 168 (1978). I do not, however, agree with the majority's reading of the record. The majority credits the seizure of the computers in this case to the "unchallenged" testimony of the searching officer and suggests that the officer's subjective knowledge that correspondence and internet searches regarding bomb materials may be found on Gall's computers prompted the seizure of the computers. In fact, the record indicates that the same officer testified that he thought it was unusual that Gall had five laptops, and sought guidance from his superiors regarding whether to seize the laptops. This testimony suggests that the searching officer suspected the laptops were stolen instead of believing that the computers were subject to seizure under the language of the search warrant. Moreover, if the computers were seized because the officer thought they were writings, then it is unclear why the police found it necessary to obtain a subsequent search warrant for the contents. Instead, if the police believed that the computers could be seized as writings, it seems likely they would have thought they could then "look" at the writings by searching the contents of the computers.

Because a computer is not analogous to a container, the seizure of a computer should

not be analyzed under the container rule. In fact, the law review article cited by the majority supports this position, specifically arguing that application of container law to computers is improper because it simplifies and inappropriately fails to recognize the distinctions between a mere container and a computer. *See Winick, supra*, at 88–89. In this article, Winick argues that courts should apply a special doctrine that has been developed by at least two jurisdictions, addressing the "intermingled document" problem, to computers. *Id.* at 104.

The intermingled document problem arises when documents subject to lawful search or seizure are intermingled with other private documents not subject to search or seizure. *Id.* The intermingled document problem has been addressed with respect to large volumes of materials only, not computers. However, the reasoning adopted to address this problem, specifically that the government can avoid violating the Fourth Amendment by sealing and holding documents pending a magistrate's approval of a further search, should be extended to computer searches. *See Tamura*, 694 F.2d at 595–97 (government can avoid violating Fourth Amendment rights by sealing documents pending issuance of search warrant detailing further search); *Shilling*, 826 F.2d at 1369 (regarding file cabinets, government should adopt the procedure outlined in *Tamura* and require *166 subsequent search warrant). Although *Tamura* and *Shilling* were not decided with respect to computers, both of these cases involved large volumes of materials, and recognized that searches authorized by warrants nonetheless raise

serious Fourth Amendment issues without special limitations. Therefore, these cases, along with Winick's article, provide guidance for handling the unique and important issues raised with respect to searches and seizures involving computers.

More recent cases have addressed the unique problems that are raised by searches of computers, and have suggested that limitations on such searches are both possible and necessary. For example, searches may be limited to avoid searching files not included in the warrant by "observing files types and titles listed in the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory." *Carey*, 172 F.3d at 1276; *see also United States v. Campos*, 221 F.3d 1143, 1147–48 (10th Cir.2000)(agreeing with *Carey* that limitations on scope of computer searches are proper under certain circumstances); Winick, *supra*, at 107.

With regard to computers, I would conclude that the particularity requirement should be more rigorous in order to protect against unreasonable governmental intrusion. Thus, I would require a search warrant seeking to seize computers or computer equipment to specify that it covers such items. Moreover, because of the inherently personal and highly complex nature of computers, I also believe that the warrant must include measures to direct the subsequent search of a computer. Thus, a warrant could specifically direct the search of the computer's contents or it could require a more specific search warrant prior to any such search. Winick, *supra*, at 103 112; *see also Davis v. Gracey*, 111 F.3d 1472

(10th Cir.1997)(separate warrant required for search of contents of computer files where computer seized pursuant to search warrant). This requirement of a separate search warrant uses the intermingled **documents** doctrine as a model, in that it limits the scope of the search of a computer's contents to that which is specifically indicated in the additional warrant, thereby avoiding a general search, which is prohibited by the Fourth Amendment.

IV.

Under the Fourth Amendment, a search warrant may not issue unless probable cause is stated within the four corners of an affidavit. Thus, the Fourth Amendment prohibits the use of information in an unsigned, unsworn search warrant to show probable cause. The affidavit in this case did not provide sufficient evidence for a magistrate to determine that there was probable cause to search any specific apartment. Furthermore, even if the information in the warrant is improperly considered along with the affidavit, there was no showing that the apartment specified was the one where it was likely that incriminating evidence might be found. Consequently, the search warrant did not properly issue, and the search here was unreasonable. I would affirm the trial court's suppression order because the evidence found pursuant to the search warrant was the product of an unconstitutional search.

Additionally, if the affidavit contained additional information and sufficiently

supported the search warrant, I would hold that the computers seized under the warrant should be suppressed. The search warrant here specified that searching officers could seize any written or printed materials, not computers. The language in the search warrant here is not sufficiently particular to include the wholesale seizure of computers, which are much more complex and versatile than mere writings. Computers should not be included within the concept of writings and should not be regarded as merely containers of writings. Instead, an affidavit in support of a warrant for the seizure of computers should clearly specify that it is requesting the seizure of computers. Moreover, a search warrant authorizing the seizure of computers should specify whether a search of the computers' data

is also authorized or whether a second warrant is necessary. In order to properly protect privacy concerns inherent in the complex nature of computers, authorization to search a computer's data should direct that search so as to avoid intrusion *167 into intermingled information that is not the subject of the search. Accordingly, I would affirm the trial court's suppression of the computers seized.

HOBBS and BENDER, JJ., join in the dissent.

All Citations

30 P.3d 145, 2001 DJCAR 1156