[Cite as *State v. Shaskus*, 2016-Ohio-7942.]

IN THE COURT OF APPEALS OF OHIO

TENTH APPELLATE DISTRICT

State of Ohio,	:	
Plaintiff-Appellant,	:	No. 14AP-812 (C.P.C. No. 13CR-4970)
v.	:	
		(REGULAR CALENDAR)
James F. Shaskus,	:	
Defendant-Appellee.	:	

D E C I S I O N

Rendered on November 29, 2016

On brief: *Ron O'Brien*, Prosecuting Attorney, and *Seth L. Gilbert*, for appellant. **Argued:** *Seth L. Gilbert*.

On brief: *Dennis C. Belli*, for appellee. **Argued:** *Dennis C. Belli*.

APPEAL from the Franklin County Court of Common Pleas

BROWN, J.

{¶ 1} This is an appeal by plaintiff-appellant, State of Ohio, from a judgment of the Franklin County Court of Common Pleas granting a motion to suppress filed by defendant-appellee, James F. Shaskus.

{¶ 2} On September 18, 2013, a Franklin County Grand Jury returned an indictment charging appellee with five counts of pandering sexually oriented matter involving a minor, in violation of R.C. 2907.322. On April 18, 2014, appellee filed a motion to suppress physical evidence and statements. Specifically, appellee sought an order from the court suppressing "the email messages under the account of jack.flash75@yahoo.com which were obtained by a detective of the Franklin County Sheriff's Department Internet Crimes Against Children Task Force from Yahoo, Inc. pursuant to a search warrant issued on October 21, 2011." Appellee also sought to

suppress "the digital images, data, and emails stored on the hard drive of the Dell desktop computer which was seized by the same detective from [appellee's] residence pursuant to a search warrant issued on November 14, 2011." On May 23, 2014, the state filed a memorandum contra appellee's motion to suppress. (Def.['s] Mot. to Suppress at 1.)

{¶ 3} On July 7, 2014, the trial court conducted a hearing on the motion to suppress. The state called as a witness David R. Hunt, formerly a detective with the Franklin County Sheriff's Department. During his employment with the sheriff's department, Detective Hunt's duties included performing investigations as part of the Franklin County Internet Crimes Against Children Task Force ("ICAC task force").

{¶ 4} At the suppression hearing, Detective Hunt provided testimony regarding a 2011 police investigation into a Craigslist advertisement soliciting sexual encounters with minors. Detective Hunt became involved in the investigation leading to the indictment against appellee as a result of "a spinoff of an investigation from another case" in which investigators "were looking at different Craigslist predators." (July 7, 2014 Tr. at 8-9.)

{¶ 5} In April 2011, a police investigator with the Franklin County Sheriff's Department became aware of an online advertisement indicating that an individual "might be seeking to have sexual encounters with minors." (July 7, 2014 Tr. at 9.) Specifically, the advertisement read: "Up to 500 younger the more u get – m4w 38. Younger the better let me take u shopping lol send pic, stats, and number! To text u." (State's Ex. A at 2.)

{¶ 6} Investigators opened an investigation and "started issuing subpoenas to various internet service providers, tracking the postings." (July 7, 2014 Tr. at 9.) According to Detective Hunt, Craigslist maintains the anonymity of posters, requiring investigators to "notify [Craigslist] with a subpoena requesting identification information" such as the internet protocol address ("IP address") used to post the advertisement. (July 7, 2014 Tr. at 10.)

{¶ 7} On September 20, 2011, Detective Hunt observed the following online Craigslist advertisement:

> [T]rade young 4 young (Columbus) I have a really young lover looking to find another guy who has the same to share. Mine is 4ft5in, 70lbs blonde, very little hair and has only been with me. If u are interested send pics, stats of yours and if I like we

> might do some trading. Or I can give benefits to u. No questions asked. I'm clean [white] and safe.

(State's Ex. B at 3.)

{¶ 8} After contacting Craigslist for information, Detective Hunt determined that an individual named Virgil Pennington had placed the advertisement linked to the email address leevp3@gmail.com, and that Pennington had an email account through America Online. Detective Hunt sought and obtained a search warrant to review other emails generated in response to Craigslist advertisements posted through Pennington's Gmail address. Specifically, on October 4, 2011, a judge from the Franklin County Municipal Court approved a warrant to Google, Inc., in California, seeking "evidence of the commission of the criminal offense of Importuning," in violation of R.C. 2907.07, to wit: "any and all emails including read, unread, and sent since September 21, 2011 and all indicia, documents, and records showing ownership or rights of possession of the email account of Virgil Pennington." (State's Ex. A at 1.)

{¶ 9} Detective Hunt obtained approximately 500 email communications sent in response to the poster of the Craigslist advertisement, including a reply by an individual who identified himself online as "Jack Flash." One of the emails from the Jack Flash email account, dated in September 2011, "included a photograph of a young, white female." The female "was fully clothed, standing in * * * a kitchen area * * * next to a birthday cake with the number '13' on it." (July 7, 2014 Tr. at 12.)

{¶ 10} In an email exchange between Flash and Pennington on September 27, 2011, Flash wrote to Pennington at the email address leevp3@gmail.com, stating: "id love if you shared yours with me but i might be able to get one for you to have as well tell me about yours." A response from leevp3@gmail.com stated: "U first. I gave mine stats now u. She has only been with me and does what * * * daddy tells her." Flash responded as follows: "mine is 4'9 and she weighs about 80lbs shes a very good girl and very accommodating do you have a pic of yours i could see? and where in columbus are you? id love to play." Pennington then wrote: "Yes pic for pic. and there will be any trading. I take urs out for a so called lunch and if all goes well Ill let u take mine out for lunch. I'm very protective of her. She is a good girl. So I also have to know u are clean and safe." Flash responded: "[P]lease send yours as well."

{¶ 11} Detective Hunt, out of concern "that there was a live victim" that he "needed to identify and locate," subpoenaed Yahoo!, Inc. ("Yahoo") to obtain the IP address information for Flash. (July 7, 2014 Tr. at 24.) The detective subsequently sought and obtained a warrant, issued by a municipal court judge on October 21, 2011, to search Yahoo for:

> [E]vidence of the commission of the criminal offenses of Compelling Prostitution, 2907.21 R.C., to wit: specifically, any and all emails including opened, unopened, sent, forwarded, deleted; any and all subscriber information including names, addresses, other email accounts; original IP address used and date the account was opened; any other information relating to the email account requested; and all indicia, documents, and records showing ownership or rights of possession of the email account of Jack Flash c/o Yahoo Inc.

(State's Ex. B at 1.)

{¶ 12} Approximately one week later, the detective received a CD from Yahoo containing "approximately 3,000 e-mails from the jack.flash75 account." (July 7, 2014 Tr. at 18.) The information included "some IP addresses as to when the account was opened," and Detective Hunt was able to determine that the Flash account was through Time Warner Cable. (July 7, 2014 Tr. at 18.) The detective sent a subpoena to Time Warner Cable, issued on November 1, 2011, "for the subscriber information for that specific IP address." (July 7, 2014 Tr. at 20.) Time Warner Cable sent Detective Hunt information that the IP address was associated with an address on Hunter Avenue, Columbus.

{¶ 13} During his review of emails, Detective Hunt found photographs of an individual he was later able to identify as appellee. The detective determined that a second individual associated with the Hunter Avenue address did not match photographs from the emails. Appellee's name eventually appeared in a public records search as an individual who also resided at the Hunter Avenue address. Based on the information obtained, the detective believed that appellee "was jack.flash75." (July 7, 2014 Tr. at 26.)

{¶ 14} Detective Hunt testified that he initially reviewed the emails from the Flash account "that only had attachments, i.e., photographs." (July 7, 2014 Tr. at 24.) During his "review of the different attachments and the earlier e-mails," Detective Hunt "came across numerous images" of what he believed to be "child pornography." (July 7, 2014 Tr. at 26.)

{¶ 15} Detective Hunt subsequently obtained a warrant to search appellee's residence on Hunter Avenue, Columbus, for evidence of pandering obscenity involving a minor, in violation of R.C. 2907.32, illegal use of a minor in nudity oriented material, in violation of R.C. 2907.323, disseminating matter harmful to juveniles, in violation of R.C. 2907.31, and endangering children, in violation of R.C. 2919.22. Detective Hunt identified state's exhibit C as the search warrant, dated November 14, 2011. At the time Detective Hunt and other officers arrived at the Hunter Avenue residence, appellee was at his workplace; Detective Hunt and another law enforcement officer went to appellee's place of employment and advised him of the nature of the warrant and "asked him if he would return home with us voluntarily or give us a key so that we could gain entry into the residence." (July 7, 2014 Tr. at 28.) Appellee accompanied the officers back to his residence.

{¶ 16} During the search, police officers recovered a computer from appellee's residence. Detective Hunt testified that a forensic examination of the computer revealed "over 900 images" of child pornography. (July 7, 2014 Tr. at 28.)

{¶ 17} Appellee testified on his own behalf during the hearing, and stated he was at work on the date the officers sought to execute the search warrant. Detectives arrived at his workplace and told him "[t]hey were getting ready to kick down the door if I would not go with them." (July 7, 2014 Tr. at 42.) Appellee testified that detectives informed him "they were looking for something in conjunction with another case. They were looking for a live person." (July 7, 2014 Tr. at 43.) One of the detectives "showed me the picture that I had shared * * * with Virgil Pennington and said do I know this person. I said no." (July 7, 2014 Tr. at 44.) Appellee acknowledged that the computers inside the house belonged to him.

{¶ 18} On July 14, 2014, the trial court conducted another hearing on the motion to suppress. At the conclusion of the hearing, the court requested the parties to brief the "specific issue of should there have been a limit on the subpoena that went to Yahoo! initially." (July 14, 2014 Tr. at 17.)

{¶ 19} On July 30, 2014, the trial court conducted a third hearing on the motion to suppress. During the hearing, the court stated on the record that it would grant the motion to suppress the email messages obtained from appellee's Yahoo account because "the search in this case was overbroad. It could have been narrow and should have been

narrow and * * * based upon that overbreadth * * * it violated Mr. Shaskus' right to his Fourth Amendment search and seizure." (July 30, 2014 Tr. at 24-25.) By decision and entry filed October 9, 2014, the trial court granted the motion to suppress.

{¶ 20} On appeal, the state sets forth the following assignment of error for this court's review:

> The Trial Court Committed Reversible Error in Sustaining Shaskus's Motion to Suppress.

{¶ 21} Under its single assignment of error, the state argues the trial court erred in granting the motion to suppress based on the court's determination that the warrant was overbroad in its authorization to search "any and all" emails without regard to date. The state maintains the warrant was based on probable cause, and that it was not overbroad.

{¶ 22} This court's review of a trial court's ruling on a motion to suppress "presents a mixed question of law and fact. When considering a motion to suppress, the trial court assumes the role of trier of fact and is therefore in the best position to resolve factual questions and evaluate the credibility of witnesses." *State v. Burnside,* 100 Ohio St.3d 152, 2003-Ohio-5372, ¶ 8, citing *State v. Mills,* 62 Ohio St.3d 357, 366 (1992). Thus, "an appellate court must accept the trial court's findings of fact if they are supported by competent, credible evidence." *Id.*, citing *State v. Fanning,* 1 Ohio St.3d 19, 20 (1982). Further, "[a]ccepting these facts as true, the appellate court must then independently determine, without deference to the conclusion of the trial court, whether the facts satisfy the applicable legal standard." *Id.,* citing *State v. McNamara,* 124 Ohio App.3d 706, 707 (4th Dist.1997). If a reviewing court "determines that a warrant should not have been issued, it must then determine whether the good-faith exception applies, and that question is a question of law, subject to de novo review by the appellate court." *State v. Castagnola,* 145 Ohio St.3d 1, 2015-Ohio-1565, ¶ 32.

{¶ 23} As noted, appellee's motion to suppress sought the suppression of evidence obtained under two search warrants, including the warrant issued by the trial court on October 21, 2011, authorizing a search of the contents of appellee's Yahoo email account. The search warrant affidavit prepared by Detective Hunt in support of that warrant application stated in part:

> Affiant, Det. David R. Hunt * * * has been with the Franklin County Sheriff's Office for over 30 years retiring in September

2011. For the past 19 years, affiant was assigned to the Special Investigations Unit conducting vice, narcotic, and internet crimes against children (ICAC) investigations.

In late September 2011, the affiant began an investigation into an individual for the internet sexual exploitation of children. This individual was posting various online ads on Craigslist looking for "young" females for sex for which he would pay for.

On Tuesday, September 20, 2011, one posting in the personals-casuals encounters was entitled:

"trade young 4 young (Columbus) I have a really young lover looking to find another guy who has the same to share. Mine is 4ft5in, 70lbs blonde, very little hair and has only been with me. If u are interested send pics, stats of yours and if I like we might do some trading. Or I can give benefits to u. No questions asked. I'm clean whaite [sic] and safe."

The affiant contacted the Franklin County Coroner's Office and provided the above noted height and weight to Chief Investigator Jack Sudimack who then plotted them on growth charts * * *. The height/weight provided on the posting would equate to a boy between the ages of 8-13 years old or a girl, 7-13 years old.

It is the affiant's training and experience that the above noted ad is consistent with that of an online child sexual predator.

On October 4, 2011, the affiant obtained a search warrant to obtain emails for the target of that investigation from Google based upon the above series of facts.

On October 12, 2011, the affiant received the requested emails from Google for the target as well as subscriber information from AOL.com for the targets account. The affiant reviewed a total of 549 emails dating from 09/21/11 to 10/04/11. One of the replies to the target was on 9/27/11 @ 1:56 PM which was an email from jack.flash75@yahoo.com to the target expressing interest in sharing his 13 y.o. daughter with the subscriber. "Jack Flash" attached a photograph of a young white juvenile female standing next to a birthday cake with the number "13" on the cake. The affiant then sent a subpoena to Yahoo to identify jack.flash75@yahoo.com.

> "Jack Flash" and the target exchanged several follow-up emails between each other from 1:56 PM and 3:17 PM. One email from "Jack Flash" stated:
>
> "mine is 4'9 and she weighs about 80lbs. shes a very good girl and very accommodating. do you have a pic of yours I could see? and where in columbus are you? I'd love to play"
>
> This description matched that of the earlier noted photograph sent by "Jack Flash" to the target.
>
> The affiant has sent an email preservation letter to Yahoo for jack.flash75@yahoo.com to save any additional emails from this person including those to possibly other suspects. The investigation into the original target of this investigation is still on-going.

(State's Ex. B at 2-3.)

{¶ 24} Based on the facts set forth in the above affidavit, a municipal court judge approved a warrant allowing access to "the email account of Jack Flash c/o Yahoo Inc." for evidence of the commission of the criminal offense of "Compelling Prostitution, 2907.21 R.C.," and authorizing the search of "any and all emails including opened, unopened, sent, forwarded, deleted; any and all subscriber information including names, addresses, other email accounts; original IP address used and date the account was opened; any other information relating to the email account requested." (State's Ex. B at 1.)

{¶ 25} The Supreme Court of Ohio has held that "[c]entral to the *Fourth Amendment* is the probable-cause requirement. While a probable-cause determination for an arrest warrant is similar in nature to that for a search warrant, a search-warrant inquiry is much more complex and presents special considerations." (Emphasis sic.) *Castagnola* at ¶ 34, citing 2 LaFave, *Search and Seizure*, Section 3.1(b) (5th Ed.2012). In order for a search warrant to issue, "the evidence must be sufficient for the magistrate to conclude that there is a fair probability that evidence of a crime will be found in a particular place. The reviewing court then must ensure that the magistrate had a substantial basis for concluding that probable cause existed." *Id.* at ¶ 35.

{¶ 26} Further, "[i]n reviewing the sufficiency of probable cause in an affidavit submitted in support of a search warrant issued by a magistrate, neither a trial court nor

an appellate court should substitute its judgment for that of the magistrate by conducting a *de novo* determination as to whether the affidavit contains sufficient probable cause upon which that court would issue the search warrant." *State v. George,* 45 Ohio St.3d 325 (1989), paragraph two of the syllabus. Rather, it is the duty of a reviewing court to simply "ensure that the magistrate had a substantial basis for concluding that probable cause existed." *Id.* Thus, "[i]n conducting any after-the-fact scrutiny of an affidavit submitted in support of a search warrant, trial and appellate courts should accord great deference to the magistrate's determination of probable cause, and doubtful or marginal cases in this area should be resolved in favor of upholding the warrant." *Id.*

{¶ 27} In the instant case, with respect to facts relevant to the issue of probable cause, Detective Hunt averred in the affidavit cited above that members of the county's ICAC task force were investigating child exploitation on the internet; specifically, an individual had posted various online advertisements on Craigslist seeking " 'young' females for sex for which he would pay for." The poster placed a personal advertisement, dated September 20, 2011, seeking to "trade young 4 young." The poster stated he had a "really young lover," described as "4ft5in, 70lbs blond," and that he was "looking to find another guy who has the same to share." The investigating detective determined that the above description would "equate" to a girl between the ages of 7 and 13 years. Detective Hunt averred that, based on his training and experience, the advertisement at issue "is consistent with that of an online child sexual predator."

{¶ 28} Detective Hunt further averred he had obtained a search warrant to obtain emails of the target of that investigation from Google. On October 12, 2011, the detective received from Google approximately 500 emails. One of the replies "was on 9/27/11 * * * which was an email from jack.flash75@yahoo.com to the target," in which the responder expressed interest in sharing his 13-year-old daughter with the subscriber. The individual, identified as "Jack Flash," had attached a photograph of a "young white juvenile female standing next to a birthday cake with the number '13' on the cake." Detective Hunt noted that Flash and the "target" had exchanged several follow-up emails, in which Flash represented that "mine is 4'9 and she weights about 80lbs." Flash further stated in the email that "shes a very good girl and very accommodating," and Flash indicated he would "love to play."

{¶ 29} In reviewing the representations in the affidavit, and considering the totality of the circumstances, we find that the affidavit gave the magistrate grounds for determining there was a fair probability that the Yahoo account of Flash contained evidence of solicitation of a minor and/or minors for sexual activity. According deference to that determination, we conclude the magistrate had a substantial basis for finding probable cause to issue the warrant to search the email account at issue.

{¶ 30} Such determination, however, does not end the inquiry into the legality of the search warrant. As noted, the focus of the trial court's analysis involved the issue of whether the warrant was overbroad. More specifically, during the suppression hearing, the court's primary inquiry was whether the absence of a temporal limitation rendered the warrant overbroad.

{¶ 31} In addition to challenging whether an affidavit provides probable cause that evidence of a crime will be found, a criminal defendant can also challenge an affidavit on the basis that it is overbroad and/or not as particular as the Fourth Amendment requires. *State v. Vu,* 9th Dist. No. 11CA-0042-M, 2012-Ohio-746, ¶ 25 (In seeking to suppress evidence, a criminal defendant "may challenge the probable cause underlying the warrant, the particularity of the warrant itself, or both.").

{¶ 32} In *Castagnola,* the Supreme Court recently considered "the application of the particularity requirement of the Fourth Amendment to the search of a computer." *Id.* at ¶ 1. Specifically, the court discussed two issues arising in the context of the particularity requirement: (1) "whether the warrant provides sufficient information to 'guide and control' the judgment of the executing officer in what to seize," and (2) "whether the category as specified is too broad in that it includes items that should not be seized." *Id.* at ¶ 79. The court further recognized, however, that "[a] search warrant that includes broad categories of items to be seized may nevertheless be valid when the description is ' " 'as specific as the circumstances and the nature of the activity under investigation permit.' " ' " *Id.* at ¶ 80, quoting *Guest v. Leis*, 255 F.3d 325, 336 (6th Cir.2001), quoting *United States v. Henson*, 848 F.2d 1374, 1383 (6th Cir.1988), quoting *United States v. Blum*, 753 F.2d 999, 1001 (11th Cir.1985).

{¶ 33} Under the facts of *Castagnola,* the defendant, Castagnola, admitted to a law enforcement official that he had damaged a prosecutor's vehicle after having looked up the address of the prosecutor on court records. A detective subsequently sought an arrest

warrant for Castagnola, as well as a warrant to search his residence. The affidavit requested a warrant to search the premises for records and documents, including those stored on computers and electronic recording devices, and further stated that any items found would be seized and used as evidence in prosecuting the crimes of "retaliation, criminal trespassing, criminal damaging, and possession of criminal tools." *Id.* at ¶ 5. A warrant was issued, leading to the seizure of numerous items, including two computers. A forensic cyber-crimes analyst, employed by the Ohio Bureau of Criminal Investigation, examined the computers through the use of a forensic software program and found a screen filled with images that she thought might be child pornography. A detective then sought a second warrant to search the contents of the computers for evidence relating to child pornography. Castagnola was subsequently indicted for ten counts of pandering sexually oriented material.

{¶ 34} Castagnola moved to suppress the evidence from the search, but the trial court denied the motion and the reviewing court affirmed. The Supreme Court accepted jurisdiction on two propositions of law, including the issue of whether a general exploratory search for evidence on a computer meets the particularity requirement of the Fourth Amendment.

{¶ 35} The Supreme Court noted under the facts of the case that the detective believed Castagnola "had found [the prosecutor's] address online and that evidence of the online search would be useful in the prosecution of the alleged offenses." *Id.* at ¶ 86. The detective testified at the suppression hearing that, in addition to a general Google or online white pages search for the prosecutor's name, he believed Castagnola may have searched a clerk of courts' website for information about the prosecutor because Castagnola mentioned in his conversation with a source that he discovered the prosecutor had received a parking ticket years earlier. The detective further testified that, "from his previous experience, he knew that an online search would create 'a cookie, which will tell you where [the persons who have used the computer] have been, what searches they have done, things of that nature.' " *Id.*

{¶ 36} The Supreme Court determined that the search warrant lacked particularity, and held that the above "details regarding the records or documents stored on the computer should have been included in the search warrant to guide and control the searcher and to sufficiently narrow the category of records or documents subject to

seizure." *Id.* at ¶ 87. The court held that "this degree of specificity was required, since the circumstances and the nature of the activity under investigation permitted the affiant to be this specific." *Id.*

{¶ 37} The *Castagnola* court also addressed the state's argument challenging "the notion that a search warrant must contain a restrictive protocol, methodology, or other strategy for conducting the search in order to satisfy the Fourth Amendment." *Id.* at ¶ 88. The Supreme Court "agree[d] that the Fourth Amendment does not require a search warrant to specify restrictive search protocols," but further "recognize[d] that the Fourth Amendment does prohibit a 'sweeping comprehensive search of a computer's hard drive.' " *Id.*, quoting *United States v. Walser*, 275 F.3d 981, 986 (10th Cir.2001). The court thus held that "[t]he logical balance of these principles leads to the conclusion that officers must describe what they believe will be found on a computer with as much specificity as possible under the circumstances," thus enabling the searcher "to narrow his or her search to only the items to be seized." *Id.* The court found this requirement "especially important when * * * the person conducting the search is not the affiant." *Id.*

{¶ 38} In general, the Warrants Clause of the Fourth Amendment "requires particularity and forbids overbreadth." *United States v. Cioffi*, 668 F.Supp.2d 385, 390 (E.D.N.Y.2009). As noted by one court, the term "overbreadth" is primarily used to refer to "authorizing seizures in excess of probable cause." *United States v. Costin*, D.C.Conn. No. 3:05-cr-38 (July 31, 2006). Some courts, however, use this term "more generally, to describe a lack of particularity." *Id.*

{¶ 39} The Supreme Court in *Castagnola* noted an overlap and interplay between "the probable-cause and particularity requirements." *Id.* at ¶ 70. Federal courts have recognized that challenges to a warrant on the grounds they are overbroad and lack sufficient particularity, while "somewhat similar in focus," involve "two distinct legal issues: (1) whether the items listed as 'to be seized' in the warrant were overbroad because they lacked probable cause and (2) whether the warrant was sufficiently particularized on its face to provide the necessary guidelines for the search by the executing officers." *United States v. Hernandez*, S.D.N.Y. No. 09-CR-625 (Jan. 6, 2010), citing *United States v. Cohan*, 628 F.Supp.2d 355, 359 (E.D.N.Y.2009) ("A warrant * * * can be unconstitutionally infirm in two conceptually distinct but related ways: either by seeking specific material as to which no probable cause exists, or by giving so vague a description

of the material sought as to impose no meaningful boundaries."). *See also In re Grand Jury Subpoenas*, 926 F.2d 847, 856-57 (9th Cir.1991) (noting that particularity and breadth are two aspects of specificity, particularity being "the requirement that the warrant must clearly state what is sought," while breadth "deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based").

{¶ 40} In the instant case, appellee argued in his motion to suppress before the trial court that the search warrant was overbroad because it "authorized the sheriff to seize 'any and all emails' in the jack.flash75@yahoo.com account," and because the warrant "did not limit the production of the emails to the particular time frame of the investigation of the September 20, 2011 Craigslist advertisement." (Appellee's Mot. to Suppress at 6.) As to the latter point, appellee argued that the detective exceeded the scope of the warrant by examining emails prior to September 2011, including a review of emails as far back as March 2009.

{¶ 41} The trial court, in granting the motion to suppress, agreed with appellee's claim that the warrant was overbroad in that it permitted the search of emails in appellee's Yahoo account without any temporal limitations. The trial court noted that investigators had "requested information from Pennington that was very limited," while "the requested information from Jack Flash was very broad." (July 30, 2014 Tr. at 25.) The court found that Yahoo "could have complied with a narrow request." (July 30, 2014 Tr. at 25.)

{¶ 42} A number of federal courts have addressed claims that the use of "any and all" language in a warrant pertaining to the search of electronic data grants the searching officer too much discretion and converts the warrant into a general warrant. The Sixth Circuit approach involves "determining reasonableness on a case-by-case basis." *United States v. Neuhard*, E.D.Mich. No. 2:15-cr-20425 (Feb. 25, 2016). *See also United States v. Richards*, 659 F.3d 527, 538 (6th Cir.2011) (noting that "the majority of federal courts have eschewed the use of a specific search protocol and, instead, have employed the Fourth Amendment's bedrock principle of reasonableness on a case-by-case basis").

{¶ 43} In this respect, federal courts have approved search warrants allowing access to the entire contents of an email account "in order to conduct a search for emails within the limited categories contained in the warrant." *In re A Warrant for All Content & Other Information Associated with the Email Account xxxxxxx@Gmail.com*

Maintained at Premises Controlled by Google, Inc., 33 F.Supp.3d 386, 394 (S.D.N.Y. 2014) (hereafter "*In re Gmail Warrant*") (noting that "every case of which we are aware that has entertained a suppression motion relating to the search of an email account has upheld the Government's ability to obtain the entire contents of the email account to determine which particular emails come within the search warrant"). *See also United States v. McDarrah,* S.D.N.Y. No. 05-CR-1182 (July 17, 2006), *aff'd* 351 Fed.Appx. 558 (2d Cir.2009) (upholding search warrant seeking "[a]ll stored electronic mail and other stored content" from AOL email account against overbreadth challenge); *United States v. Upham,* 168 F.3d 532, 535 (1st Cir.1999) (court finding, in case involving search of computer for images of child pornography on computer, that affidavit requesting "[a]ny and all" computer disks and disk drives "was about the narrowest definable search and seizure reasonably likely to obtain the images"); *United States v. Deppish,* 994 F.Supp.2d 1211, 1215 (D.C.Kan.2014) (upholding warrant requiring "all contents" of Yahoo account for evidence of crimes of sexual exploitation of minors); *Richards* at 539 (upholding search of defendant's entire internet server and noting that, in "[a]pplying a reasonableness analysis on a case-by-case basis, the federal courts have rejected most particularity challenges to warrants authorizing seizure and search of entire personal or business computers").

{¶ 44} Regarding search warrant challenges based on the lack of temporal limitations, the absence of a date limitation may render a warrant overbroad or insufficiently particular. *See United States v. Ford,* 184 F.3d 566, 576 (6th Cir.1999) ("Failure to limit broad descriptive terms by relevant dates, when such dates are available to the police, will render a warrant overbroad."). Federal courts, however, appear to generally agree that temporal restrictions are not mandatory. *See United States v. DSD Shipping, A.S.*, S.D.Ala. No. 15-00102-CG-B (Sept. 2, 2015) ("Defendants cite no binding precedent to support the assertion that temporal restrictions are a mandatory requirement of a digital search. Rather, * * * courts consider the totality of the circumstances and in some cases, find that a temporal restriction is part of a series of factors considered rather than a threshold requirement."); *United States v. Triumph Capital Group,* 211 F.R.D. 31, 58 (D.C.Conn.2002) ("A temporal limitation in a warrant is not an absolute necessity, but is only one indicia of particularity," and therefore "the

absence of a temporal limitation does not render the warrant a prohibited general warrant.").

{¶ 45} Cases in which federal courts have upheld search warrants in the absence of temporal limitations typically look to the nature and circumstances of the criminal activity, as well as a consideration of whether the warrant was "already adequately particularized." *United States v. Capote*, N.D.Ga. No. 1:15-CR-00338-MHC-CMS (May 5, 2016) ("Because the warrant in this case was already sufficiently particularized based on the subject matter limitation—i.e., evidence relating to the criminal activity under investigation—the lack of an additional time period limitation in the warrant does not render the search unconstitutional."); *United States v. Ali El Khateeb*, M.D.Fla. No. 8:14-cr-00185-T-23MAP (Aug. 4, 2015), quoting *United States v. Smith*, 918 F.2d 1501, 1507-08 (11th Cir.1990) (rejecting claim that warrant's failure to specify a date range rendered it fatally overbroad and defective for the seizure of any emails; rather, because the warrant "limits the seizure of electronic information to that connected with the possession, receipt, and distribution of controlled substances," such " 'nexus' satisfies the practical realities 'that enable the searcher to ascertain and identify things authorized to be seized' "); *United States v. Lee*, N.D.Ga. No. 1:14-CR-00227-TCB-RGV (July 6, 2015) (rejecting argument that issuance of a search warrant requiring Google to disclose the contents of any electronic communications or files belonging to the relevant account did not satisfy Fourth Amendment's particularity requirement; investigative agents "had 'good reason not to include a temporal limitation in the warrants,' since they did not know, when they obtained the warrants, whether [an internet website] existed in some other form at the time the accounts were first opened in 2004").

{¶ 46} Federal courts have rejected the necessity for temporal limitations in cases involving the search of computers for child pornography, noting the particular difficulties posed in such cases. *See, e.g., Deppish* at 1220 (finding that "[a] temporal limitation was not reasonable because child pornography collectors tend to hoard their pictures for long periods of time," and further noting "the dynamic nature of email accounts makes it more difficult to limit the scope of emails to particular dates"); *United States v. Adams*, D.C.Ver. No. 2:14-cr-79 (Aug. 25, 2015) (rejecting claim, in child pornography case, that warrant was overbroad because it did not constrain the search to a particular time frame, and distinguishing between cases involving business records and electronically stored

child pornography; "there is often no way around the fact that many image files will have to be viewed to ensure that no relevant evidence has been missed").

{¶ 47} Ohio courts have also considered the issue of temporal limitations in the context of the search of electronic devices. In *State v. McCrory*, 6th Dist. No. WD-09-074, 2011-Ohio-546, ¶ 38, the court noted the general rule adopted by federal courts that "[t]he absence of a temporal limitation will not automatically render the warrant a prohibited general warrant." Rather, "[a] temporal limitation in a warrant is merely one indicium of particularity." *Id.* (Collecting federal authorities; citations omitted.)

{¶ 48} Under the facts of *McCrory*, a detective investigated allegations by a woman that the appellant had sexually assaulted her at his residence after she responded to an advertisement on "craigslist.org for a topless maid." *Id.* at ¶ 2. A municipal judge issued three search warrants based on facts in the detective's affidavit indicating that evidence of rape would be found on the appellant's home computers and peripheral devices. The appellant, who was subsequently charged with gross sexual imposition and pandering sexually oriented material involving a minor, filed a motion to suppress evidence seized from his home computer.

{¶ 49} One of the warrants issued in that case authorized the police "to analyze the seized devices and 'recover any emails, documents, photos, or any other documentation pertaining to Craigslist.org, the victim from 08-6911, any phone calls, text messages received or made to the victim of 08-6911 * * * which is in violation of 2907.02 ORC Rape.' " *Id.* at ¶ 9. The trial court denied the motion to suppress and, on appeal, the appellant raised a challenge that the warrants were insufficiently particular and overbroad because "they described the items to be seized in broad terms without imposing a temporal limitation." *Id.* at ¶ 32. More specifically, the appellant argued that "a 'narrower description was available to the police, namely a limitation to the time between the [Craigslist] ad placement (June 14, 2008) and the complaint (June 28, 2008).' " *Id.* at ¶ 33.

{¶ 50} The reviewing court in *McCrory* rejected the appellant's argument, finding that the lack of temporal limitations did not render the warrants overbroad because the warrants "contained sufficient subject-matter limitations to satisfy the particularity requirement." *Id.* at ¶ 34. The court noted that "[s]ubject-matter limitations sufficient to

satisfy the particularity requirement include references to the crime or criminal activity at hand, specific persons, or specific types of materials." *Id.* at ¶ 43.

{¶ 51} In the present case, based on this court's review of the record and applicable law, we conclude that the warrant authorizing the search of appellee's Yahoo email account was not overbroad or insufficiently particular. We have previously determined that the magistrate had a substantial basis for finding probable cause to permit the search of the account for evidence of solicitation of a minor and/or minors for sexual activity. The warrant at issue specifically identified the email account to be searched and limited the scope of the search to evidence of a particular crime, i.e., "evidence of the commission of the criminal offense of Compelling Prostitution, [R.C.] 2907.21." *See Deppish* at 1220 (while affidavit sought disclosure of entire Yahoo email account, it "limited seizure to instrumentalities and evidence tending to show and identify persons engaged in" a specific offense, i.e., "sexual exploitation of children in violation of 18 U.S.C. § 2252(a)"). *See also United States v. Tsarnaev*, 53 F.Supp.3d 450, 457 (D.C.Mass.2014) (the scope of the warrant was properly limited by "restricting the search to evidence of specified crimes"); *State v. Enyart*, 10th Dist. No. 08AP-184, 2010-Ohio-5623 ¶ 40 (search warrant not overbroad where it "named the items to be seized in reference to the crimes of voyeurism and pandering, thus limiting the search to items related to the offense").

{¶ 52} The fact that the warrant in this case authorized the search of "any and all" emails in the account did not render it impermissibly overbroad or facially invalid. As noted, federal courts have in general upheld the government's ability to "obtain the entire contents" of an email account in order to determine "which particular emails come within the search warrant." *In re Gmail Warrant* at 394 (collecting cases; citations omitted.) *See also United States v. Grimmett*, 439 F.3d 1263, 1271 (10th Cir.2006) (warrant authorizing agents to search "any and all" computer equipment was not overbroad because it contained "sufficiently particularized language requiring a nexus with child pornography").

{¶ 53} Nor do we find the lack of a temporal limitation to be dispositive under the circumstances. As cited above, courts have generally determined there is no blanket requirement that warrants have a date restriction. During the suppression hearing in this case, Detective Hunt testified that he was concerned there was "a live victim that was being molested in real time" (i.e., a minor being traded for sex) that he needed to identify

and locate. (July 7, 2014 Tr. at 13.) As noted by the state, one of the emails from Flash, and identified in the affidavit, stated that the girl he was offering to trade for sex was "a very good girl and very accommodating," suggesting that Flash had traded the minor for sex in the past. The detective also averred in the affidavit that he sent Yahoo a preservation letter to save additional emails from this individual, including those to "possibly other suspects," and that the investigation was "still on-going."

{¶ 54} Thus, at the time of the affidavit, investigators knew that an individual using a Yahoo email account and the moniker "Jack Flash" had responded to an advertisement by a poster seeking to "trade young 4 young," and that Flash in turn had offered to trade a minor for sex; the ICAC task force, however, did not have information regarding the identity of Flash or the girl, and whether Flash had previously arranged through emails to trade the girl for sex. The state argues that, based on the information available at the time, including language in the emails suggesting Flash had traded an "accommodating" minor in the past, Detective Hunt had a valid reason not to include a temporal limitation. We agree and find it was reasonable for the magistrate reviewing the affidavit to conclude that emails in the Yahoo account predating the exchanges between Flash and Pennington might contain evidence relating to solicitation of a minor. *See United States v. McDarrah,* 351 Fed.Appx. 558, 561 (2d Cir.2009) (rejecting claim that warrant to search entire contents of AOL account was overbroad as not limited to email messages between defendant and "Julie" or "David Smith"; magistrate "could have determined there was ample evidence that a crime was committed and strong indication that further evidence of criminal activity could be found in e-mails between McDarrah and people other than 'Julie' and 'David Smith' "); *Richards* at 541 ("In light of the information known at the time the search warrant was issued," warrant authorizing search of entire server was not overbroad.); *Lee* (even though certain emails may have "predated the alleged onset" of criminal activity, such emails "might nevertheless prove relevant" in determining the identity of the defendants involved, and could be important for "authenticating the evidence and laying a proper foundation"). Based on the record presented, we conclude that the warrant in this case was " ' "as specific as the circumstances and the nature of the activity under investigation permit[ted]." ' " *Castagnola* at ¶ 80, quoting *Leis* at 336, quoting *United States v. Henson,* 848 F.2d 1374, 1383 (6th Cir.1988), quoting *United States v. Blum*, 753 F.2d 999, 1001 (11th Cir.1985).

{¶ 55} Additionally, we note that Detective Hunt testified that he conducted the search of the email account employing a limiting methodology. Specifically, the detective performed a filtering procedure by restricting his review of the emails to those with attachments, hoping to discover the identity of the 13-year-old girl depicted in the photograph in the email sent by appellee. *See, e.g.*, *Deppish* at 1220 (although warrant did not identify a particularized search strategy, agent employed such a strategy; "[h]e did not search or view the entirety of the emails in the YAHOO account," but, rather, he "performed a keyword, filtered search, to focus on those emails that would probably contain instrumentalities and evidence * * * tending to show and identify persons engaged in sexual exploitation of children"). *See also Grimmett* at 1270 (even though warrant authorized search of "any and all computer software," there was no evidence of "exploratory rummaging" as agent "testified that he specially searched for files with images," and thus "[n]o wholesale searching occurred here, despite the broad authority the warrant may have granted"). Similarly, the facts of this case do not suggest evidence of such "exploratory rummaging," nor does the record indicate the search method employed by the detective was unreasonable.

{¶ 56} On review, we do not find that the search warrant at issue was impermissibly overbroad or that it was particularly insufficient. Accordingly, we conclude that the trial court erred in granting appellee's motion to suppress evidence with respect to the search of appellee's Yahoo email account.

{¶ 57} Appellee has submitted, as supplemental authority, the Supreme Court's recent decision in *Castagnola*. We find, however, the facts of that case, as well as the particularity concerns addressed therein, are distinguishable and do not compel a determination that the search warrant at issue in this case was invalid.

{¶ 58} In general, *Castagnola* stands for the proposition that "[t]he particularity demanded from a search warrant is contingent upon the government's knowledge and the particular circumstances of the case." *State v. Knoefel*, 11th Dist. No. 2014-L-088, 2015-Ohio-5207, ¶ 129, citing *Castagnola* at ¶ 80. As noted in our earlier discussion of *Castagnola*, the Supreme Court, in finding that the language of the search warrant did not "guide and control" the judgment of the forensic examiner, cited testimony by the examiner that "Castagnola's computer was brought in for a case involving 'menacing, threatening, and intimidation,' " and that the "analyst read the case synopsis and the

search-warrant affidavit and then looked at all the information on the hard drive 'looking for any evidence of intimidation of David * * * and anything associated with that.' " *Id.* at ¶ 83. The court found "the determination on what to seize was within [the forensic examiner's] discretion." *Id.* Further, the broad language of the warrant permitted the forensic examiner "to examine every record or document on Castagnola's computer in order to find any evidence of the alleged crimes." *Id.* at ¶ 84. Noting testimony by the detective as to his knowledge of Castagnola's online activities in seeking information about the law director, as well as the detective's general knowledge about an online search creating a "cookie," the Supreme Court found "those details regarding the records or documents stored on the computer should have been included" in the search warrant to guide and control the searcher because "the circumstances and the nature of the activity under investigation permitted the affiant to be this specific." *Id.* at ¶ 86, 87.

{¶ 59} By contrast, the investigators in the present case did not possess that type of knowledge and information. Stated otherwise, under the facts of *Castagnola*, the police were "capable of providing greater particularity" based on the amount of knowledge they possessed regarding the object of the search. *Knoefel* at ¶ 129 (distinguishing the facts of *Castagnola*). Additionally, the concerns raised by the scope of the search conducted under the facts of *Castagnola* (permitting the forensic examiner "to examine every record or document on Castagnola's computer in order to find any evidence of the alleged crimes") are not present in the instant case. *Castagnola* at ¶ 84. As previously noted, the warrant at issue in this case authorized police to search for evidence related to a specific offense, and Detective Hunt limited his review of the emails to those with attachments, hoping to discover the identity of the 13-year-old girl described by appellee in the email he sent to Pennington.[1]

[1] We note that the facts of the instant case, in which the detective who submitted the affidavit was involved in the investigation and search, do not raise an additional concern noted by the Supreme Court in *Castagnola* regarding scenarios in which a mistaken search can occur where "the person conducting the search [i.e., the forensic analyst] is not the affiant." *Castagnola* at ¶ 88.

{¶ 60} Based on the foregoing, we conclude that the trial court erred in granting appellee's motion to suppress evidence seized from his Yahoo email account.[2] We therefore sustain the state's single assignment of error.

{¶ 61} Accordingly, having sustained the state's assignment of error, the judgment of the Franklin County Court of Common Pleas is reversed, and this matter is remanded to that court for further proceedings in accordance with law, consistent with this decision.

Judgment reversed and cause remanded.

DORRIAN, P.J., concurs.
BRUNNER, J., dissents.

BRUNNER, J., dissenting.

{¶ 62} I respectfully dissent from the decision of the majority. I would overrule the State's sole assignment of error and affirm the judgment of the trial court. I would hold that a search warrant based on a single suspicious e-mail conversation that purported to authorize the search of any and all e-mails regardless of sender, recipient, subject, date, or status (opened, unopened, deleted, sent, or forwarded) or duration of e-mail account was unconstitutionally overbroad. The executing officer (who was also the affiant for the search warrant) was not justified in relying on it. I would hold that the fruits of that search and other derivative searches traceable to such a warrant were properly excluded.

{¶ 63} In considering whether a warrant is unconstitutionally overbroad, reviewing courts must conduct a de novo review. *State v. Dingess*, 10th Dist. No. 10AP-848, 2011-Ohio-5659, ¶ 32, citing *State v. Enyart*, 10th Dist. No. 08AP-184, 2010-Ohio-5623, ¶ 38; *State v. Gritten*, 11th Dist. No. 2004-P-0066, 2005-Ohio-2082, ¶ 11; *United States v. Ford*, 184 F.3d 566, 575 (6th Cir.1999).

{¶ 64} The authority for finding a warrant overbroad finds its origins in the plain text of the Fourth Amendment.

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

[2] The trial court did not reach the merits of appellee's constitutional challenge to the second warrant, authorizing the search of the Hunter Avenue residence. We leave it to the trial court to decide in the first instance, on remand, that issue.

> and *particularly describing the place to be searched, and the persons or things to be seized*.

(Emphasis added.) "It is familiar history that indiscriminate searches and seizures conducted under the authority of 'general warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment." *Payton v. New York*, 445 U.S. 573, 583 (1980); *see also id.* at 583-85, fn. 21, quoting *Stanford v. Texas*, 379 U.S. 476, 481-82 (1965); *Boyd v. United States*, 116 U.S. 616, 625 (1886). "[S]earches deemed necessary should be as limited as possible. [T]he problem is not that of intrusion *per se*, but of a general, exploratory rummaging in a person's belongings." (Emphasis sic.) *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). This Court has observed, " '[t]o search for evidence of a crime there must "be a nexus * * * between the item to be seized and criminal behavior" as well as "cause to believe that the evidence sought will aid in a particular apprehension or conviction." ' " *Dingess* at ¶ 33, quoting *Enyart* at ¶ 32, quoting *Warden, Maryland Penitentiary v. Hayden*, 387 U.S. 294, 307 (1967).

{¶ 65} The majority decision spends significant effort in discussing and distinguishing the recent Supreme Court of Ohio decision finding that a warrant that purported to authorize a search of a computer was insufficiently particular where it failed to limit the search within the computer to particular subjects and sought instead merely "[r]ecords and documents stored on the computer." *State v. Castagnola*, 145 Ohio St.3d 1, 2015-Ohio-1565, ¶ 77. In reaching this finding, the Supreme Court explained:

> Courts addressing the particularity requirement of the Fourth Amendment are concerned with two issues. The first issue is whether the warrant provides sufficient information to "guide and control" the judgment of the executing officer in what to seize. *United States v. Upham*, 168 F.3d 532, 535 (1st Cir.1999). The second issue is whether the category as specified is too broad in that it includes items that should not be seized. See *United States v. Kow*, 58 F.3d 423, 427 (9th Cir.1995).
>
> A search warrant that includes broad categories of items to be seized may nevertheless be valid when the description is " ' "as specific as the circumstances and the nature of the activity under investigation permit." ' " *Guest v. Leis*, 255 F.3d 325, 336 (6th Cir.2001), quoting *United States v. Henson*, 848 F.2d 1374, 1383 (6th Cir.1988), quoting *United States v. Blum*, 753 F.2d 999, 1001 (11th Cir.1985). Warrants that fail to

> describe the items to be seized with as much specificity as the government's knowledge and the circumstances allow are "invalidated by their substantial failure to specify as nearly as possible the distinguishing characteristics of the goods to be seized." *United States v. Fuccillo*, 808 F.2d 173, 176 (1st Cir.).
>
> Because computers can store a large amount of information "there is a greater potential for the 'intermingling' of documents and a consequent invasion of privacy when police execute a search for evidence on a computer. * * * Officers must be clear as to what it is they are seeking on the computer and conduct the search in a way that avoids searching files of types not identified in the warrant." *United States v. Walser*, 275 F.3d 981, 986 (10th Cir.2001). "[P]ractical accuracy rather than technical precision" is the operative consideration. *United States v. Dorrough*, 927 F.2d 498, 500 (10th Cir.1991).

Castagnola at ¶ 79-81. The Supreme Court also explained the fact that the records "would be used to prosecute Castagnola for the crimes of retaliation, criminal trespassing, criminal damaging, and possession of criminal tools, added nothing to narrow the search." *Id.* at ¶ 82. "As written," the Court concluded, "this search warrant failed to address both concerns that courts consider when determining whether a warrant satisfies the particularity requirement of the Fourth Amendment." *Id.*

{¶ 66} In judging the validity of a warrant we are limited to the information that was presented to the magistrate which, in cases without a hearing, confines our analysis to the four corners of the warrant affidavit. *Castagnola* at ¶ 39; *State v. Bean*, 13 Ohio App.3d 69, 71 (6th Dist.1983). Here the warrant affidavit set forth the facts known to the police that justified the suspicion that evidence of a crime might be found at Yahoo!, Inc. ("Yahoo") as follows:

> [The target of another investigation, on] Tuesday, September 20, 2011, [posted an advertisement on Craigslist:]
>
> "trade young 4 young (Columbus) I have a really young lover looking to find another guy who has the same to share. Mine is 4ft5in, 70lbs blonde, very little hair and has only been with me. If u are interested send pics, stats of yours and if I like we might do some trading. Or I can give benefits to u.No questions asked. I'm clean whaite and safe."
>
> * * *

> One of the replies to the target was on 9/27/11 @ 1:56 PM which was an email from jackflash75@yahoo.com to the target expressing interest in sharing his 13 y.0. daughter with the [target]. "Jack Flash" attached a photograph of a young white juvenile female standing next to a birthday cake with the number "13" on the cake.
>
> "Jack Flash" and the target exchanged several follow-up emails between each other from 1:56 PM and 3:17 PM. One email from "Jack Flash" stated:
>
> "mine is 4'9 and she weighs about 80lbs. shes a very good girl and very accommodating. do you have a pic of yours i could see? and where in columbus are you? id love to play"
>
> This description matched that of the earlier noted photograph sent by "Jack Flash" to the target.

(Sic passim.) (State's Ex. B at 2-3.) Based on this information, Detective Hunt sought and obtained a warrant to search Yahoo and seize, "any and all emails including opened, unopened, sent, forwarded, deleted [as to] the email account of Jack Flash," as well as information regarding "other email accounts." *Id*. at 2.

{¶ 67} Like computers, e-mail accounts "can store a large amount of information" and thus, as is true of computer searches, " 'there is a greater potential for the "intermingling" of documents and a consequent invasion of privacy when police' " seek to search through a person's e-mails. *Castagnola* at ¶ 81, quoting *United States v. Walser*, 275 F.3d 981, 986 (10th Cir.2001). Consequently, "[o]fficers must be clear as to what it is they are seeking" and avoid seizing or searching "types [of e-mails] not identified in the warrant." *Id*. Applying the reasoning set forth by *Castagnola* to this case, the warrant sought and obtained by Detective Hunt was insufficiently particular to satisfy constitutional requirements. The warrant affidavit presented evidence that "Jack Flash" had responded to an advertisement one afternoon in September 2011 that appeared to propose the exchange of juvenile children for sexual purposes. The affidavit presented no evidence to suggest that "Jack Flash" had followed through on the trade or that the would-be crime actually materialized past the planning stages, nor did it present any evidence

that "Jack Flash" had ever attempted such a trade before.[3] "Jack Flash's" description of a girl as "very accommodating" implied that he had some experience with her willingness to engage in sexual behavior. (State's Ex. A at 6.) But the affidavit did not explain why evidence of "Jack Flash's" sexual activities with this girl would be contained in e-mails, let alone explain the need to seize every e-mail "opened, unopened, sent, forwarded, [or] deleted" from "Jack Flash's" e-mail account regardless of subject, sender, or recipient for the entire history of the account's existence or why information about "other email accounts" would be pertinent. (State's Ex. B at 2.)

{¶ 68} In short, like the warrant in *Castagnola*, the warrant here does not "guide and control" the judgment of the executing officer in what to seize (because it essentially commands the officer to seize everything), and the category as specified is too broad in that it includes items that should not be seized (thousands of unrelated and irrelevant private communications). *Castagnola* at ¶ 79, citing *United States v. Upham*, 168 F.3d 532, 535 (1st Cir.1999); *United States v. Kow*, 58 F.3d 423, 427 (9th Cir.1995). This warrant, which purported to authorize the seizure of literally every e-mail to pass through the jack.flash75 account for the entire duration of the account's existence, irrespective of sender, recipient, or subject, was the quintessential "general, exploratory rummaging in a person's belongings." *Coolidge* at 467.

{¶ 69} The State argues that the broad scope of the warrant was justified by the need to determine "whether, when, how often, and with whom 'Jack Flash' had offered up the girl for sex in the past, and any other children involved." (State's Brief at 9.) However, the concept that "Jack Flash" had ever "offered up [this] girl for sex in the past, and any other children," is post hoc speculation unsupported at its inception by an evidentiary basis. *Id.* at 9. The affidavit contains no factual information that "Jack Flash" had used e-mail to offer this girl or any other children for sex before, and the affiant did not offer an opinion based on a factual reason to suspect that he had. (State's Ex. B at 2.)

{¶ 70} Warrants issue upon probable cause, and the basis for probable cause is fact, not speculation. *Miller v. Sanilac Cty.*, 606 F.3d 240, 248 (6th Cir.2010), quoting *Henry v. United States*, 361 U.S. 98, 102 (1959) (defining probable cause as "when 'the facts and circumstances * * * warrant a prudent [person] in believing that an offense has

[3] Shaskus apparently did not actually have a daughter and stated he had no idea who the girl was in the

been committed.' "). The speculation that the State proposes to indulge is little different from arguing that there is probable cause to search the house of a suspected burglar for the loot of other, different burglaries on the theory that if a burglar has committed one burglary, he must have committed others.

{¶ 71} The reasons supporting probable cause must be contained in the warrant affidavit. It is not sufficient to offer them for the first time (such as in a suppression hearing or an appellate brief) long after the warrant has been executed. *Castagnola* at ¶ 39; *Bean* at 71. Only by post hoc speculation could one conclude from the warrant affidavit that "Jack Flash's" e-mails (other than e-mails related by time, senders, or subjects, to the conversation that justified the search warrant) would show evidence of other crimes. (State's Ex. B at 2-3.)

{¶ 72} The State argues that the warrant was justified by the need to determine the identity of the girl in the photograph and the need to determine "Jack Flash's" identity. I acknowledge that it was important to the investigation to attempt to discern the identity of "Jack Flash" and his purported "daughter." However, "Jack Flash's" identity (and the identity of his "daughter") could have been readily ascertained by requesting records from Yahoo regarding the IP address and identity of the owner of the e-mail account. In fact, in addition to the request for "all emails," the warrant specifically sought exactly those records from Yahoo. It was through "Jack Flash's" IP address, not his e-mails, that the residence was located. Courts have discouraged the practice of using the search for background investigative facts as a justification for searches beyond the scope of probable cause. *Ford* at 576; *United States v. Srivastava*, 476 F. Supp.2d 509, 514 (D.Md.2007).

{¶ 73} Even assuming the validity of the State's basis for a warrant authorizing a broader search of the e-mails, the scope of the warrant was still too broad. In *United States v. Abboud*, 438 F.3d 554, 575-76 (6th Cir.2006), the United States Sixth Circuit Court of Appeals found a warrant was overbroad where it sought records from a six-year time span when the facts in the affidavit only evidenced a check-kiting scheme spanning three months. *Id.* (ultimately finding the error was harmless). The Sixth Circuit has moreover explained, "[f]ailure to limit broad descriptive terms by relevant dates, when such dates are available to the police, will render a warrant overbroad." *Ford* at 576.

---

picture with the cake and "13" candle. (State's Ex. A at 7.)

{¶ 74} In this case the *evidence* for the search warrant consisted of one conversation related to a Craigslist advertisement between two persons on the afternoon of September 27, 2011. Yet, the *warrant* authorized the search and seizure of "all emails" regardless of date, subject, sender, or recipient, "opened, unopened, sent, forwarded, [or] deleted," and it even authorized the collection of records relating to "other email accounts." (State's Ex. B at 2.) Depending on the age of the jack.flash75 account, the warrant could have authorized the seizure of decades of e-mail. The record does not reflect how old the jack.flash75@yahoo.com address was, but it is undisputed that "well over 3,000 emails" were seized. (State's Ex. C at 5.) In the "well over 3,000 emails" the police found just one culpable conversation involving child pornography in March 2009—two and one-half years before the Craigslist conversation that purported to justify the search. *Id.*

{¶ 75} The majority notes that the officer somewhat limited his examination of the e-mails by examining only those that had attachments. (Majority decision at ¶ 14.) The majority also states that, "federal courts have approved search warrants allowing access to the entire contents of an email account 'in order to conduct a search for emails *within the limited categories contained in the warrant*.' " (Emphasis added.) (Majority decision at ¶ 43, quoting *In re A Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx@Gmail.com Maintained at Premises Controlled by Google, Inc.*, 33 F.Supp.3d 386, 394 (S.D.N.Y.2014)). However, I would respectfully view those observations as a whole as a proverbial red herring, because Shaskus' case does not involve a large volume of e-mails that were copied and then reviewed according to limitations set forth in a warrant, but rather, a large volume of e-mails seized with no such limitations in the warrant.

{¶ 76} I acknowledge that in the context of electronic records, the police may sometimes end up with a copy of an account because perhaps a third-party custodian (like Yahoo) will not wish to search through the e-mail account itself in order to identify materials implicated by a limited warrant even though authorized to do so. But regardless of whether Yahoo or any other similarly situated custodian makes a copy of the entire account, makes a copy of part of the account, or invites the police on-site to inspect material in its data center, in order to be constitutionally valid, the warrant must still direct the police as to what material to search and seize as evidence. The mere fact that

the nature of electronic records dictates that they reside with a third party and that it is sometimes more practical to search a copy in the police station rather than search the original at the data center, does not mean that the warrant authorizing and limiting the search is relieved of the particularity requirements of the Fourth Amendment. As the Sixth Circuit Court of Appeals in *Ford*, put it, "[f]ailure to limit broad descriptive terms by relevant dates, when such dates are available to the police, will render a warrant overbroad." *Id*. at 576. In other words, where, as here, the police know what time-frame is involved, they cannot constitutionally ignore the limits of probable cause and instead seek and act on a warrant with unlimited broad descriptive terms. Because if a warrant is based on probable cause as to a limited time frame but authorizes unlimited search and seizure, it is overbroad.

{¶ 77} The evidence seized (e-mails and attachments) during the search of Yahoo was appropriately suppressed. *See United States v. Wong Sun*, 371 U.S. 471, 487-88 (1963). The trial court was also justified in suppressing the evidence found on Shaskus' computer during the search of his residence. The warrant to search Shaskus' residence authorized a search of "a computerized information system" to discover "evidence of the commission of the criminal offenses of Pandering Obscenity Involving a Minor, 2907.32 R.C.; Illegal Use of a Minor in Nudity Oriented Material, 2907.323 R.C.; Disseminating Matter Harmful to Juveniles, 2907.31 R.C.; [and] Endangering Children, 2991.22 R.C. " (State's Ex. C at 1.)

{¶ 78} The motivator for the search of Shaskus' house and computer was finding child pornography, extended from the original suspicion that Shaskus had a daughter whom he was attempting to trade for sex. The pornography found on Shaskus' computer was "fruit of the poisonous tree." It was found during a search of computer equipment and supported by the child pornography evidence obtained in the unconstitutionally overbroad search of Yahoo. *Id*. at 487-88. As the Supreme Court of Ohio held:

> The exclusionary rule reaches not only primary evidence obtained as a direct result of an illegal search or seizure, but also evidence later discovered and found to be derivative of an illegality, or "fruit of the poisonous tree." *Nardone v. United States* (1939), 308 U.S. 338, 60 S.Ct. 266, 84 L.Ed. 307. The reason for the rule is the concern that if derivative evidence were not suppressed, police would have an incentive to violate constitutional rights in order to secure admissible derivative

> evidence even though the primary evidence secured as a result of the constitutional violation would be inadmissible. *See* Katz, *Ohio Arrest, Search and Seizure* (3 Ed.1992), Section 2.07. Justice Frankfurter explained in *Nardone*, "To forbid the direct use of methods thus characterized but to put no curb on their full indirect use would only invite the very methods deemed 'inconsistent with ethical standards and destructive of personal liberty.'" *Nardone, supra,* at 340, 60 S.Ct. at 267, 84 L.Ed. at 311.

State v. Carter, 69 Ohio St.3d 57, 67 (1994).

{¶ 79} The majority decision does not reach the State's good-faith argument, because it reverses the trial court's decision. That argument should be addressed, because of its tendency to be used incorrectly to excuse an unconstitutional search and seizure in violation of the Fourth Amendment. The State argues that the police relied in good faith on warrants to search both Yahoo and Shaskus' home and computer. That is, the State contends that an exception to the exclusionary rule arises because the officers relied in good faith on the warrants, and the evidence therefore should not have been excluded. *Id.*; *United States v. Leon*, 468 U.S. 897 (1984).

{¶ 80} However, the "good faith" exception to the exclusionary rule set forth in *Leon* does not operate where "a warrant [is] so facially deficient -- *i.e.*, in failing to particularize the place to be searched or the things to be seized -- that the executing officers cannot reasonably presume it to be valid." *Id.* at 923; *see also, e.g., Gritten* at ¶ 20. Here, the Yahoo warrant purported to authorize the seizure of "any and all emails" for the entire account history irrespective of sender, recipient, or subject and whether the e-mails were "opened, unopened, sent, forwarded, [or] deleted," and it even extended to the collection of records relating to "other email accounts." (State's Ex. B at 2.) Absent evidence of pervasive, continuous, and long-standing use of this and other e-mail accounts for criminal activity, this warrant was facially overbroad; it was so much so that Detective Hunt (who was the affiant and thus knew that the evidence justifying the warrant consisted of a single suspicious conversation on a single afternoon between just two persons) could not have reasonably presumed it to be valid.

{¶ 81} With respect to the warrant to search Shaskus' computer and home, the Supreme Court has held, "[t]he good-faith exception does not apply where a search warrant is issued on the basis of evidence obtained as a result of an illegal search." *Carter*

at 68. Were the rule otherwise, an officer could violate the United States Constitution to obtain incriminating evidence, "launder" that evidence by presenting it to a magistrate in order to obtain a warrant for a further search, and then rely on the good faith of officers executing the warrant to avoid the exclusion of incriminating evidence found pursuant to the warrant search. *See Nardone v. United States*, 308 U.S. 338, 340-41 (1939); *see also, e.g.*, *Murray v. United States*, 487 U.S. 533, 540 (1988); *Carter* at 67.

{¶ 82} For the reasons set forth in this dissent, I would overrule the State's sole assignment of error and affirm the judgment of the trial court.
