THIRD DIVISION
ELLINGTON, P. J.,
BETHEL and GOBEIL, JJ.

June 27, 2018

In the Court of Appeals of Georgia

A18A0659. MADDOX v. THE STATE.

GOBEIL, Judge.

Following a bench trial in Cobb County Superior Court, James Maddox was convicted of two counts of distributing child pornography and two counts of possessing child pornography. Maddox now appeals from the denial of his motion for a new trial, arguing that the trial court erred in admitting a written document provided police by Maddox's Internet service provider ("ISP") in response to a subpoena. He further contends that in the absence of that document, the evidence was insufficient to convict him of distributing child pornography. Additionally, Maddox claims that even if the subpoenaed document was admissible, the evidence failed to prove that he distributed child pornography and the trial court therefore erred in denying his motion for a directed verdict on the distribution charges. And Maddox also asserts

that the trial court erred in denying his motion to suppress: (1) the subscriber information obtained through an allegedly illegal subpoena served on his ISP; (2) evidence obtained during a search of Maddox's residence pursuant to a warrant; and (3) incriminating statements Maddox made during his initial police interview. For reasons explained below, we find no error and affirm.

"On appeal from a criminal conviction, the defendant is no longer entitled to a presumption of innocence and we therefore construe the evidence in the light most favorable to the jury's guilty verdict." *Marriott v. State*, 320 Ga. App. 58, 58 (739 SE2d 68) (2013) (citation omitted). So viewed, the record shows that this case involves the distribution of child pornography through a peer-to-peer file sharing program, which represents a commonly used method of obtaining and sharing child pornography. Such programs allow the sharing of digital media and documents between computers. One of these peer-to-peer programs, known as ARES, is available for any member of the public to download from the Internet. When ARES downloads, it automatically installs on the user's desktop a folder that is identified as "My Shared Folder." Other ARES users are then able to access, view, and download any document or digital media stored in the shared folder of another ARES

user.[1] Additionally, when an ARES user downloads information from the shared folder of another ARES computer, the items downloaded will automatically be stored in the user's shared folder. If a user wants to prevent downloaded items from being accessed and downloaded by others, he or she can move those files out of the shared folder, delete the files, disconnect his or her computer from the Internet, or uninstall the peer-to-peer file sharing program.

Once a person has downloaded the ARES program, he or she can use it to search for specific terms. The program will then compile a list of other ARES users whose shared folders contain filenames that include one or more of those search terms. The user then has the ability to download those "matching" files, which will automatically be stored in his or her computer's shared file folder.[2]

In or about May 2013, the Cobb County Police Department was investigating the ARES peer-to-peer file sharing program to determine if anyone in Cobb County was distributing child pornography using the ARES network. The Cobb County

---

[1] ARES does not allow a user to see anything on another computer that is not stored in the shared folder.

[2] One of the investigating officers testified that in his experience, people interested in obtaining and exchanging child pornography have chat rooms and "other areas" on the Internet where they can discuss file names. People can then run ARES searches based on this information.

Police Department ran on one of its secure computers a program called Round Up ARES ("RU-ARES"). The program searched other ARES computers for terms associated with child pornography.[3] The RU-ARES program also ran a search for videos and pictures using a secure hash algorithm, also known as an SHA-1. Based on the number and arrangement of pixels, every video and picture has a specific SHA-1 value. Thus, the RU-ARES program in this case searched for the SHA-1 values of specific images and videos known to contain child pornography. Additionally, the search was limited to IP addresses that were potentially located in Cobb County.

On May 22, 2013, the RU-ARES program running on the police department's computer identified an IP address in Cobb County as having six shared files that contained possible child pornography. Three files were downloaded to the police department computer from that IP address on May 22, a fourth file downloaded on May 23, and a fifth file downloaded on May 29. Sergeant Raymond Drew of the Cobb

[3] These terms included "PTHC" (which stands for "preteen hard-core"); Lolita; LS Magazine (a known child pornography magazine); and any number less than 18 accompanied by the letters "YO" (the "YO" standing for "years old").

County Police Department[4] reviewed those files after they were downloaded and determined that each of them contained what appeared to be child pornography. Working with a crime analyst, Drew learned that the ISP for the IP address in question was Comcast. Drew then prepared a grand jury subpoena for Comcast asking them to produce the subscriber name, physical address, and other identifying information for the IP address in question. . The subpoena was served on Comcast and the ISP provided law enforcement with information showing that the account in question belonged to Maddox and that the bills went to a residential address in Marietta.

Upon learning that the computer using the IP address was associated with a residence inside the Marietta city limits, Drew provided all of the information regarding the investigation to Detective Mark Erion with the City of Marietta Police Department. The information provided to Erion included Maddox's subscriber information and a copy of the downloaded files. After determining that Maddox lived at the residential address in question, Erion obtained a search warrant for that

[4] At the time, Sergeant Drew was a detective in the Crimes against Women and Children Unit.

residence. During the execution of the search warrant, police located three computers, including a Dell desktop and a Dell laptop, both of which belonged to Maddox.

At the time the search warrant was executed, Maddox agreed to talk with police and an audio recording of this interview was admitted and played at trial. . During that interview, Maddox, who had majored in computer science, told police that he had downloaded the ARES software so that he could obtain pornography from the Internet. Maddox explained that any pornographic files he downloaded went to the "My Shared Folder" on his desktop, and that he was the only person who had downloaded anything to his computers. Additionally, Maddox admitted that he located the titles of and previewed the pornographic files before downloading them, and he admitted to downloading all of the files subsequently obtained by the State using RU-ARES. Maddox further admitted that he was aware that child pornography videos were in his shared folder, but stated that he was drunk at the time he downloaded them.

Police obtained a search warrant for Maddox's computers, and a forensic examination of those computers showed the presence of child pornography on both the desktop and the laptop. The desktop contained a total of 19 videos containing child pornography, including the five videos transferred to the State's computer

during the RU-ARES search. A shared folder on the laptop held approximately 13 videos containing what appeared to be child pornography.

Maddox was indicted on five counts of distributing child pornography based on the five videos in his desktop's "My Shared Folder" that were downloaded to the State's computer. He was also indicted on two counts of possessing child pornography, based on a video and an image found on his laptop. Prior to trial, Maddox moved to suppress the subscriber information provided by Comcast, the search warrants for Maddox's residence and his computers, and Maddox's incriminating statements made during his police interview. . Following a full evidentiary hearing, the trial court denied that motion. The case then proceeded to a bench trial at which the court found Maddox guilty of two counts of distributing child pornography and two counts of possessing child pornography, but acquitted him of the three remaining distribution charges.[5] The trial court subsequently denied Maddox's motion for a new trial, and Maddox now brings this appeal.

1. In response to the subpoena requesting Comcast to provide subscriber information related to the IP address from which police downloaded pornographic

[5] Maddox was acquitted of counts 2, 4, and 5 of the indictment based on the State's failure to prove beyond a reasonable doubt that the persons in the videos serving as the basis for those counts were under the age of 18.

videos, Comcast provided a written document containing the requested information. When the State introduced this document into evidence at trial, defense counsel objected "on the grounds that it's not the best evidence. [It's] a facsimile transmittal. . . . [A]nd it's hearsay as well. And I . . . object to it on the previous Fourth Amendment grounds [asserted] in the motion to suppress." The trial court overruled the objection and allowed the State to introduce the document under OCGA § 24-8-803 (6) as a business record. Maddox challenges this ruling on appeal.

Georgia Rule of Evidence 803 (6) provides that the following shall be admissible as an exception to the hearsay rule:

> Records of regularly conducted activity. Unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness . . . *a memorandum, report, record, or data compilation, in any form*, of acts, events, conditions, opinions, or diagnoses, if (A) made at or near the time of the described acts, events, conditions, opinions, or diagnoses; (B) made by, or from information transmitted by, a person with personal knowledge and a business duty to report; (C) kept in the course of a regularly conducted business activity; and (D) it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness or by certification that complies with paragraph (11) or (12) of Code Section 24-9-902 . . .

OCGA § 24-8-803 (6) (emphasis supplied).

Here, the State used a Rule 902 (11)[6] certification for the Comcast document. Specifically, attached to the document was a "Business Record Certification," executed by a Comcast employee who identified himself as a custodian of records. The certification stated that the responsive document constituted a record generated and kept in the ordinary course of Comcast's business; that it was made at or near the date reflected in the document; that it was made by someone with personal knowledge of the information contained therein; and that it was kept in the course of regularly conducted activity as a regular practice of Comcast. Given these facts, we find no abuse of discretion by the trial court in finding that the requirements of Rule 803 (6) were met and that the Comcast document was admissible as a business record. See *Roberts v. Comm. & S. Bank*, 331 Ga. App. 364, 369 (2) (771 SE2d 68) (2015) (we review a trial court's ruling as to the admissibility of a document as a business record only for an abuse of discretion).

On appeal, Maddox asserts that the Comcast document did not qualify for admission under Rule 803 (6) because it was not a business record but instead was

[6] Under Rule 902 (11), a party may use a written certification of the record's custodian to meet the requirements of Rule 803 (6) (A)-(C). See OCGA § 24-9-902 (11).

a summary of information found in Comcast's business records. Maddox also contends that the document did not qualify under Rule 803 (6) because it was created in response to a subpoena and therefore was not prepared in the normal course of business. Maddox, however, failed to assert these specific grounds below for excluding the evidence, either before or after the trial court found that the document qualified for admission under the business record exception. Accordingly, we find that this claim of error has been waived.

Georgia law requires that to preserve a claim of error related to the admission of evidence, a party must assert "a timely objection . . . stating the specific ground of objection, if the specific ground was not apparent from the context." OCGA § 24-1-103 (a) (1). And we have interpreted this Code section to mean that a party must apprise the trial court of the basis for the objection with sufficient particularity to allow an informed decision to be made on the legal issue involved. See *Powell v. State*, 335 Ga. App. 565, 568 (2) (782 SE2d 468) (2016) ("[t]he trial court must have the opportunity to be fully informed of the [alleged] error and rule on it"); *Ruffin v. State*, 333 Ga. App. 793, 794 (2) (777 SE2d 262) (2015) ("[t]o fully inform the trial court and permit a ruling, the defendant must articulate the specific basis for objecting to the [evidence]") (citation and punctuation omitted); *Sowell v. State*, 327 Ga. App.

532, 536 (1) (759 SE2d 602) (2014) (finding that defendant waived his claim that a document was not properly authenticated when he failed to make such an objection at trial). On appeal, therefore, we may not consider any grounds for admitting or excluding evidence that were not asserted in the trial court. *Powell*, 335 Ga. App. at 568 (2). This rule results from the fact that "[a]n issue that is not presented or ruled on by the trial court is not preserved for appellate review." *Anthony v. State*, 302 Ga. 546, 549 (II) (807 SE2d 891) (2017) (holding that although defendant had objected at trial to the introduction of the photographic lineup, he "did not specifically raise the issue of whether the photographic lineup procedures were flawed" and therefore the issue was "not preserved for [appellate] review"). See also *Ward v. State*, 339 Ga. App. 621, 622 (1) (794 SE2d 246) (2016) ("[w]here an entirely different objection or basis for appeal is argued in the brief which was not presented at trial we will not consider that basis as we are limited to those grounds presented to and ruled upon by the trial court") (citation and punctuation omitted).

Here, Maddox objected to the evidence on the grounds that it was hearsay, and the trial court thereafter indicated it was admitting the document under the hearsay exception found in Rule 803 (6). Maddox made no further objection, and did not raise either of the arguments he now seeks to raise on appeal. Specifically, Maddox failed

to argue that the document did not qualify for admission as a business record either because it constituted a summary of other business records or because it was not created in the normal course of business. Given that "[Maddox's] objection was not sufficient to notify the trial court of the additional legal grounds he now asserts as his basis for appeal, and [that Maddox] sought no ruling from the court on those objections . . . [Maddox] has waived his grounds for appeal on this issue." *Powell*, 335 Ga. App. at 568 (2).

2. Maddox argues that because the Comcast document constituted inadmissible hearsay, the State failed to prove he was guilty of distributing child pornography. Specifically, Maddox contends that absent the Comcast document, the State had no proof that it was Maddox's computer connected to the IP address from which the State downloaded pornography. In light of our holding in Division 1, this argument is without merit.

3. Maddox next contends that the trial court erred in denying his motion for a directed verdict on the charges of distribution. A trial court may grant a directed verdict "only when all of the reasonable deductions and inferences arising from the undisputed evidence demand a finding that the accused is not guilty" of the charged crimes. *Battles v. State*, 273 Ga. 533, 533 (2) (543 SE2d 724) (2001).

(a) Maddox was convicted under Georgia's Child Exploitation Statute, OCGA § 16-12-100, which makes it "unlawful for any person knowingly to create, reproduce, publish, promote, sell, distribute, give, exhibit, or possess with intent to sell or distribute any visual medium which depicts a minor or a portion of the minor's body engaged in any sexually explicit conduct." OCGA § 16-12-100 (b) (5). To the extent that Maddox is contending that the term "distribute" does not encompass his conduct in making pornographic material available for others to download, we disagree.

Although OCGA § 16-12-100 (a) defines a number of terms, "distribute" is not one of them. And the current case appears to represent the first time this Court has been called on to interpret the language of the Child Exploitation Statute. To ascertain the meaning of "distribute" in this context, therefore, we apply settled and familiar canons of statutory interpretation. We look first to the "plain and ordinary meaning" of the term "distribute." *Deal v. Coleman*, 294 Ga. 170, 172 (751 SE2d 337) (2013). See also *Warren v. State*, 294 Ga. 589, 590 (755 SE2d 171) (2014) (we must look to the General Assembly's understanding of the "ordinary meaning" of the statutory language "at the time [it] enacted the statute"); OCGA § 1-3-1 (b) ("[i]n all interpretations of statutes, the ordinary signification shall be applied to all words").

And we read the text of the entire statute together, in the "most natural and reasonable way, as an ordinary speaker of the English language would." *Deal*, 294 Ga. at 172-173.

When looking for the generally understood or common meaning of a particular word, courts most often look to dictionary definitions. See, e. g., *Abdel-Samed v. Dailey*, 294 Ga. 758, 763 (2) (755 SE2d 805) (2014); *Warren*, 294 Ga. at 590-591. Black's Law Dictionary defines distribute as meaning "[t]o deliver" or "[t]o spread out; to disperse." Black's Law Dictionary 508 (10th ed. 2014). Similarly, Merriam-Webster provides this definition of distribute: "to divide among several or many . . . to spread out so as to cover something . . . to give out or deliver especially to members of a group." Merriam-Webster N. D., Merriam-Webster.com. (Accessed 15 June 2018). Given the commonly understood meaning of "distribute," we find that where, as here, an individual knowingly makes materials available for others to take and those materials are in fact taken, distribution has occurred. As now Justice Gorsuch explained when writing for the Tenth Circuit and construing a substantially similar federal statute concerning child pornography:

> [Although the defendant] may not have actively pushed pornography on [other users of the peer-to-peer file sharing program], . . . he freely

> allowed them access to his computerized stash of images and videos and openly invited them to take, or download, those items. It is something akin to the owner of a self-serve gas station. The owner may not be present at the station, and there may be no attendant present at all. And neither the owner nor his or her agents may ever pump gas. But the owner has a roadside sign letting all passersby know that, if they choose, they can stop and fill their cars for themselves, paying at the pump by credit card. Just because the operation is self-serve . . . we do not doubt for a moment that the gas station owner is in the business of "distributing," "delivering," "transferring[,]" or "dispersing" gasoline; the raison d'être of owning a gas station is to do just that. So, too, a reasonable [factfinder] could find that [the defendant] welcomed people to his computer and was quite happy to let them take child pornography from it.

United States v. Shaffer, 472 F3d 1219, 1223-1224 (1) (10th Cir. 2007). See also *United States v. Stitz*, 877 F3d 533, 538 (III) (C) (4th Cir. 2017) ("where files have been downloaded from a defendant's shared folder, use of a peer-to-peer file-sharing program constitutes 'distribution'" under federal law); *United States v. Richardson*, 713 F3d 232, 236 (II) (5th Cir. 2013) ("we conclude that downloading images and videos containing child pornography from a peer-to-peer computer network and storing them in a shared folder accessible to other users on the network amounts to distribution under [federal law]"); *United States v. Budziak*, 697 F3d 1105, 1109 (II)

(9th Cir. 2012) (evidence "that the defendant maintained child pornography in a shared folder, knew that doing so would allow others to download it, and another person actually downloaded it" showed that defendant had distributed child pornography); *United States v.Chiaradio*, 684 F3d 265, 282 (II) (E) (1st Cir. 2012) ("[w]hen an individual consciously makes files available for others to take and those files are in fact taken, distribution has occurred"); *United States v. Spriggs*, 666 F3d 1284, 1287 (11th Cir. 2012) (finding that the distribution element of a federal law imposing an enhanced sentence for distributing child pornography is satisfied where defendant posts "illicit images on a publicly accessible website" or "makes the files accessible to others" by "placing them in a file sharing folder"); *United States v. Collins*, 642 F3d 654, 656-657 (II) (8th Cir. 2011) (evidence that defendant used a file-sharing program supported his conviction for knowing distribution of child pornography).

Here, Maddox admitted that he downloaded the ARES program onto his computer and that he understood that file sharing was the purpose of that program. He also admitted that he had child pornography stored in his computer's shared folder. Additionally, Maddox could have, but did not, move his downloaded images and videos into a computer folder that was not subject to file sharing. And Cobb

County police were able to download images and videos from the child pornography collection in Maddox's shared folder. Under these facts, the evidence supported the factfinder's conclusion that Maddox had distributed child pornography.

(b) Despite the foregoing, Maddox contends that subsection (d) of the Child Exploitation Statute immunizes him from criminal liability for any conduct that might otherwise be considered the distribution of child pornography. That statutory subsection provides that OCGA § 16-12-100 (b) (which criminalizes, among other things, the reproduction, publishing, exhibition, and distribution of child pornography) "shall not apply to . . . [t]he activities of law enforcement and prosecution agencies in the investigation and prosecution of criminal offenses[.]" OCGA § 16-12-100 (d) (1). Maddox argues that because the distribution in this case took place in the context of a police investigation, that distribution was not subject to prosecution under OCGA § 16-12-100 (b). We disagree.

Reading subsection (d) in the "most natural and reasonable way, as an ordinary speaker of the English language would," *Deal*, 294 Ga. at 172-173, its language provides immunity from criminal prosecution for any law enforcement officer or prosecutor who, in the course of fulfilling his or her duties, engages in conduct that might otherwise constitute a violation of the Child Exploitation Statute. To be entitled

to this immunity, however, two requirements must be satisfied. First, the person asserting immunity must be a member of a law enforcement or prosecution agency. Second, the otherwise illegal conduct must have occurred when that person was acting in their official capacity to investigate and/or prosecute a violation of OCGA § 16-12-100. Here, given that Maddox can satisfy neither of these requirements, he is not entitled to the immunity offered under OCGA § 16-12-100 (d).

4. The subpoena served on Comcast seeking Maddox's subscriber information was issued pursuant to OCGA § 24-13-21 (e), which allows a district attorney to issue a subpoena in grand jury proceedings. On appeal, Maddox asserts that such subpoenas are not a valid method for obtaining subscriber information from an ISP. Instead, Maddox contends that such information can be obtained only where a law enforcement agency or district attorney's office complies with the requirements of OCGA § 16-9-109.[7] And because the subpoena at issue did not comply with this

[7] That statute provides, in relevant part:

> Any law enforcement unit, the Attorney General, or any district attorney may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service, exclusive of the contents of communications, only when any law enforcement unit, the Attorney General, or any district attorney: (A) Obtains a search warrant as

statute, Maddox argues that the trial court erred when it denied his motion to suppress the information produced by Comcast.

We need not decide in this case whether OCGA § 16-9-109 provides the exclusive mechanism through which law enforcement and prosecutorial agencies may obtain subscriber information from an ISP. This is because a party seeking to suppress evidence must demonstrate that he has standing to do so. See *Courtney v. State*, 340 Ga. App. 496, 497 (797 SE2d 496) (2017). And Maddox lacks standing to object to the legality of a search of Comcast's records. As we have explained previously, the customer of an ISP has no reasonable expectation of privacy in the subscriber information the customer voluntarily conveys to the ISP. *Ensley v. State*, 330 Ga. App. 258, 259 (765 SE2d 374) (2014). Accordingly, a customer cannot bring a Fourth Amendment challenge to any subpoena or warrant served on the ISP that seeks the customer's subscriber information. Id.

> provided in Article 2 of Chapter 5 of Title 17; (B) Obtains a court order for such disclosure under subsection (c) of this Code section; or (C) Has the consent of the subscriber or customer to such disclosure.

OCGA § 16-9-109 (b) (1).

Although Maddox concedes that he lacks standing to challenge the subpoena at issue on Fourth Amendment grounds, he argues that OCGA § 16-9-109 (d) (4) provides him with such standing. We disagree. This Court has previously considered and rejected the argument that OCGA § 16-9-109 provides an Internet subscriber with standing to challenge a request for information served on the subscriber's ISP. See *Courtney*, 340 Ga. App. at 499. In *Courtney*, a criminal defendant charged with distribution of child pornography sought to challenge an administrative subpoena for subscriber information served on his ISP. The trial court denied the defendant's motion to suppress and the defendant appealed, arguing that OCGA § 16-9-109 (b) provided him with standing to challenge the subpoena because that statutory subsection "defines the circumstances under which an [ISP] may be compelled to disclose [subscriber] information to a law enforcement agency." Id. at 497. We rejected that assertion, reasoning that although

> OCGA § 16-9-109 (b) sets forth the process by which a district attorney may require an [ISP] to disclose certain subscriber information[,] . . . [n]othing in this Code section prohibits the [ISP] from disclosing the information to the district attorney, law enforcement, the Attorney General, or for that matter, anyone else.

Id. at 499 (punctuation and citation omitted). Accordingly, we found that the statute granted the defendant neither a reasonable expectation of privacy in his subscriber information nor standing to challenge a subpoena seeking that information. Id.

We find that the same logic applies to Maddox's argument that OCGA § 16-9-109 (d) (4) provides him with standing to challenge the subpoena at issue in this case. Subsection (d) outlines the requirements *for admissibility* of any evidence produced by an ISP under subsections (a), (b), or (c) of OCGA § 16-9-109. See OCGA § 16-9-109 (d) (1)-(4). And subsection (d) (4) provides:

> No later than 30 days prior to trial, a party intending to offer such evidence produced in compliance with this subsection shall provide written notice of such intentions to the opposing party or parties. A motion opposing the admission of such evidence shall be filed within 10 days of the filing of such notice, and the court shall hold a hearing and rule on such motion no later than 10 days prior to trial. Failure of a party to file such motion opposing admission prior to trial shall constitute a waiver of objection to such records and affidavit. However, the court for good cause shown, may grant relief from such waiver.

OCGA § 16-9-109 (d) (4). Thus, while subsection (d) might provide a party with a basis for objecting to the admissibility of certain evidence, it does not provide a party with standing to object to a subpoena served on his or her ISP. Accordingly, we find

no error by the trial court in denying Maddox's motion to suppress the subscriber information obtained from Comcast.

5. Maddox asserts that the trial court erred in refusing to suppress the evidence obtained pursuant to the search warrant for his residence and his incriminating statements made to police, as all of that evidence is the fruit of the illegal subpoena served on Comcast. In light of our holding in Division 4, these claims of error are without merit.

For the reasons set forth above, we affirm the denial of Maddox's motion for new trial.

Judgment affirmed. Ellington, P. J., and Bethel, J., concur.