NUMBER 13-19-00504-CR

COURT OF APPEALS

THIRTEENTH DISTRICT OF TEXAS

CORPUS CHRISTI – EDINBURG

ANTONIO SALINAS, **Appellant,**

v.

THE STATE OF TEXAS, **Appellee.**

On appeal from the 406th District Court of Webb County, Texas.

OPINION

Before Chief Justice Contreras and Justices Longoria and Tijerina
Opinion by Chief Justice Contreras

Appellant Antonio Salinas appeals the denial of his motion to suppress following his convictions for two counts of possession of child pornography, a third-degree felony. *See* TEX. PENAL CODE ANN. § 43.26(a). By three issues, Salinas argues the trial court should have suppressed the evidence because (1) its admission violates the Texas exclusionary rule; (2) its admission violates the United States Constitution and the Texas

Constitution; and (3) there were false or reckless statements included in a search warrant affidavit. We affirm.

I. BACKGROUND[1]

On August 26, 2017, Salinas was indicted on thirty-five counts of possession of child pornography. *See id.* He filed a motion to suppress the evidence underlying his offenses, arguing that: (1) the evidence was obtained by a private person in violation of the law; (2) law enforcement performed an illegal warrantless search; and (3) the search warrants were invalid because their supporting affidavits contained materially false information and omitted information in reckless disregard for the truth.

After a hearing, the trial court denied the motion and issued findings of fact and conclusions of law. The trial court's findings of fact provided:

> 1. On June 12, 2017, Antonio Salinas, dropped off his Ford F150 pickup at Sames Motor Company to perform a diagnostic because the "check engine" light was on, the air conditioner was blowing hot air[,] and part of the glove compartment was detached. In the ordinary course of business, [the] Sames [car dealership] obtained Antonio Salinas's authorization and signature on Sames' "Service Drive Quick Write Up" form that included the following language: "DISCLAIMER: It is understood that this company assumes no responsibility [sic] for loss or damage to this vehicle or its contents. Permission is granted to operate this vehicle on any street or road for the *purpose of testing or inspection* [emphasis added]. Authorization for labor and materials is granted and an express mechanic's lien is hereby acknowledged to secure payment." Signs inside the warehouse and elsewhere on the premises stated Sames was not responsible for lost or stolen items.
>
> 2. Sames Motor Co. issues an "Employee Handbook" to all employees and obtains signatures attesting they will abide by the policies. Sames has employee policies including a requirement that employees follow all laws and regulations and should have the highest standards of conduct and personal integrity and further advises the employees to turn over valuable

[1] This case is before this Court on transfer from the Fourth Court of Appeals in San Antonio pursuant to a docket-equalization order issued by the Supreme Court of Texas. *See* TEX. GOV'T CODE ANN. § 73.001.

or dangerous property to the appropriate manager for safe keeping if the employee observes such property when caring for a customer's vehicle.

3. Alberto Luna, Octavio Limon[,] and Eden Salinas[2] were service mechanics employed by Sames Motor Co. and each signed acknowledgment of policies.

4. Approximately two hours after dropping his truck off at Sames, [Salinas] returned to recover his laptop. [Salinas] personally retrieved his computer laptop from inside the truck.

5. [Limon] was authorized to use his personal computer at Sames and was provided with the necessary licensed software to conduct any diagnostics. On June 13, 2017, [Limon], while performing diagnostics on the truck from the truck's driver seat, connected his computer to the truck's port. [Eden], a technician whose dock neighbored Limon's, approached the open driver's side door to talk to Limon. [Salinas] noticed some Splenda packets located in the driver's door open compartment. Salinas the[n] noticed a USB[3] device among the Splenda packets. The [thumb drive] was not connected or interconnected to any computer or device and was not marked with any identifying marks or names. Curious to find out if there was any music on it, [Eden] asked [Limon] to look into the [thumb drive].

6. Upon plugging in the [thumb drive], [Limon] was able to access images in a file entitled "ZZZZ"; the [thumb drive] did not have a password and was not encrypted. Limon, sitting directly in front of his laptop, saw thumbprints[4] of images depicting what he believed were minor girls in sexual poses with

---

[2] Eden Salinas is unrelated to appellant. We will refer to this technician by his first name to avoid confusion.

[3] "USB" stands for "universal serial bus," and it is a "standardized serial computer interface that allows simplified attachment of peripherals especially in a daisy chain." MERRIAM-WEBSTER'S ONLINE DICTIONARY, https://www.merriam-webster.com/dictionary/USB (last visited Apr. 14, 2021); *see Advanced Micro Devices, Inc. v. LG Electronics, Inc.*, No. 14-CV-01012-SI, 2017 WL 1383271, at *5 (N.D. Cal. Apr. 18, 2017) (order) (noting that each USB device comprises a plurality of "independently operating endpoints" that transmit and receive data between the USB device and the USB host). The USB device here was a thumb drive. A thumb drive is an external portable storage device for computers. *See* MERRIAM-WEBSTER'S ONLINE DICTIONARY, https://www.merriam-webster.com/dictionary/flash-drive (last visited Apr. 14, 2021); MERRIAM-WEBSTER'S ONLINE DICTIONARY, https://www.merriam-webster.com/dictionary/thumb-drive (last visited Apr. 14, 2021); *see also United States v. Capozzi*, No. 3:16CR347, 2019 WL 1330440, at *2 (M.D. Pa. Mar. 25, 2019) ("A thumb drive is a portable, computer, storage device."); *United States v. LaPradd*, No. 3:10-CR-00076-R, 2010 WL 3853140, at *1 (W.D. Ky. Sept. 28, 2010) ("A thumb drive is an external memory storage device for computers similar to a floppy disk, only smaller and with more memory-storage capability.").

[4] The trial court clearly meant "thumbnails." *See Thumbnail*, WIKIPEDIA, https://en.wikipedia.org/wiki/thumbnail (last visited Apr. 19, 2021) ("Thumbnails are reduced-size versions of pictures or videos, used to help in recognizing and organizing them.").

little to no clothing. [Eden], standing by the open driver's door, also observed the images.

7. Shocked, [Eden] informed [Luna] that he and [Limon] had observed child pornography when looking into a [thumb drive] they obtained from a truck Limon was servicing, and asked Luna for help in deciding what action to take, if any. Luna contacted a friend, who recommended they report their discovery to the police right away. [Luna] called 911 and reported the discovery of child pornography because [Limon] and [Eden] were afraid of losing their jobs. Although [Luna] was not involved in servicing [Salinas's] truck and did not personally observe the child pornography, he injected himself into the story when he [falsely] told the 911 operator and the first arriving officer, Officer David Paz [that he saw the images of child pornography while using the [thumb drive] as part of the inspection and work on the vehicle].[5]

8. Upon Officer Paz'[s] arrival at approximately 10:43 a.m., [Luna] informed Officer Paz that he and [Eden] were working on a truck and while checking to see if the truck's USB port was properly working, they connected a [thumb drive] that was in the vehicle to determine whether it was the USB port or the USB device that was not working[, and] they plugged the USB device into Limon's computer and discovered images of child pornography. Officer Paz was unaware of the employee policy and believed that Luna was being truthful about what was seen on the [thumb drive]. Officer Paz had no cause to believe that the testimony given by Luna, as to the reason for viewing the [thumb drive], was untrue. Officer Paz acted on the information obtained by the Sames' employees with a good faith belief of its veracity.

9. Alberto Luna identified the truck where the [thumb drive] was found and further handed the [thumb drive] to Officer Paz. Officer Paz held the [thumb drive] and asked Luna to show him what they had found. Luna, Limon[,] and [Eden] led Officer Paz to Limon's computer and connected the [thumb drive] to Limon's computer and showed Officer Paz where the child pornographic images had been discovered by them.

10. Officer Paz observed the images and confirmed that the [thumb drive] had approximately 7 images of young females without any clothing between

[5] All three men testified that the information they gave to 911 and the police concerning the reason they accessed the thumb drive was false. Limon and Eden explained at the hearing on the motion that they accessed the thumb drive out of curiosity and not because there were any issues related to any of the thumb drive connections in the truck. Both Limon and Eden stated that looking through Salinas's thumb drive was not necessary for any reason related to the inspection or repair of the vehicle, and all three men testified that Luna did not work on the vehicle and was not present when Limon and Eden accessed the thumb drive. All three men testified that Limon and Eden reached out to Luna afterwards and that they fabricated the story told to police that they were working on the USB port on the vehicle when they accessed Salinas's thumb drive. The men explained they fabricated the story because they were afraid of losing their jobs and because Eden and Limon were worried about talking to the police.

the ages of 11 and 14 exposing breasts and vaginal area. Officer Paz then removed the [thumb drive], contacted his sergeant and waited for his arrival.

11. When Sergeant Edgar Garza and Special Victim's Sergeant Cordelia Perez arrived, Officer Paz again connected the [thumb drive] to Limon's computer and showed them where the child pornography images were located. Thereafter, Detective Charlie Rosales arrived on the scene, where he spoke to [Limon] and obtained written consent from Limon to take Limon's computer for forensic analysis, along with the [thumb drive] containing child pornography.

12. Based on the foregoing, on June 14, 2017, Laredo Police Department Special Investigations Unit ("SVU") Detectives applied for a search warrant to conduct a forensic analysis on the [thumb drive] and Limon's computer. SVU detectives then obtained two additional search warrants to search Dr. Salinas'[6] office . . . and Dr. Salinas' home . . . .

13. On June 22, 2017, SVU attempted to execute the search warrant of Dr. Salinas'[s] home . . . . Dr. Salinas was not at home at that time. Investigator Rosales called Dr. Salinas on his mobile phone and Dr. Salinas agreed to meet with Investigator Rosales at Doctor's Hospital. At the hospital, Investigator Rosales advised Dr. Salinas of the investigation and search warrants. More specifically, Investigator Rosales advised Dr. Salinas that they had found child pornography on his [thumb drive] taken from his vehicle. Investigator Rosales further advised Dr. Salinas that because of what was found on the [thumb drive], he had obtained search warrants for Dr. Salinas'[s] home, office, and electronic mobile devices. Investigator Rosales explained to Dr. Salinas that the device that downloaded the illicit images found on his [thumb drive] and his mobile phone were subject to the search warrants. Dr. Salinas led Investigator Rosales to a private room and unlocked the door so he and Rosales could speak. Dr. Salinas then tendered his Laptop computer and cell phone to SVU detectives. Dr. Salinas agreed to meet Investigator Rosales at LPD headquarters in his own vehicle. Before going to LPD headquarters, no law enforcement officers followed Dr. Salinas to LPD headquarters.

14. At LPD headquarters, after being advised of the warrants and details of the investigation, Dr. Salinas asked Investigator Rosales if he was going to be arrested. Investigator Rosales told Dr. Salinas that if he was compliant and answered all of Investigator Rosales'[s] questions, he would not be arrested and could go home. Investigator Rosales then read Dr. Salinas his Miranda warnings and Dr. Salinas answered Investigator Rosales' questions in a recorded interview. During the interview, Dr. Salinas was equivocal about the [thumb drive], saying he did not remember it or that he forgot about any [thumb drive] containing child pornography. Dr. Salinas

[6] At the time of his arrest, Salinas was a licensed medical doctor.

> further detailed how he became involved in viewing these images and videos of child pornography, the frequency of his viewing of child pornography[,] and that he possessed additional child pornography on his computers and other USB [devices]. After the interview, Dr. Salinas was allowed to go home but was advised that LPD would be seeking a warrant authorizing his arrest for possession of child pornography. On June 23, 2017, Dr. Salinas was arrested pursuant to images found on the [thumb drive] for possession of child pornography.
>
> 15. The forensic analysis of [Limon's] computer and the [thumb drive] indicated that the [thumb drive] was initially accessed at 9:52 a.m. and last accessed at 12:10 p.m. on June 13,2017. Only two folders existed in the USB device-"iPhotos" and "ZZZZ" subfolders with no other images or documents in the root. Limon and [Eden] would have seen an image of seven thumb[nail] images of child pornography.

The trial court issued the following conclusions of law:

> 1. [Salinas] failed to establish a violation of Texas Penal Code *§32.02.* The USB [thumb drive] is not a "computer" device and was not connected or related to a computer device in which [Salinas] had an expectation of privacy. Tex. Penal Code Ann. § 33.01.
>
> 2. Officer Paz'[s] viewing of the [thumb drive's] content was not a search under the Fourth Amendment of the United States Constitution because Paz'[s] viewing was confirmatory in nature, as it did not exceed the scope of the initial viewing by Sames' employees. *Us. Const. amend. IV.* See *United States v. Barth,* 26 *FSupp.2d* 929 *at 937.*
>
> 3. The search by Officer Paz did not require a search warrant because [Limon] consented to the search of the [thumb drive] while attached to Limon's computer. Limon's consent was valid because Sames-and by extension its employees-had joint access and control over [Salinas's] truck and its contents. See *Welsh v. State,* 93 *SW3d* 50 *(2002),* citing *United States v. Matlock,* 415 U.S. 164,94 S.Ct. 988, 39 L.Ed.2d 242 (1974). At the time that the Sames' employees initially viewed the images on the [thumb drive,] they were not acting in concert with the police or for investigative purposes.
>
> 4. The confirmatory search of the [thumb drive] by Officer Paz allowed a valid warrantless seizure of the device because it contained contraband (i.e., child pornography), in plain view, and thus allowed for the [thumb drive's] immediate seizure by Officer Paz. See *Joseph v. State, 807* S.W.2d. *303* (Tex.Crim.App.1991); *State v. Hailey,* 811 S.W.2d 597 (Tex.Crim.App.1991)

5. Any subsequent viewing by LPD Officers does not constitute a search under the Fourth Amendment because it was confirmatory in nature, as it did not exceed the scope of the initial viewing by Sames' employees. See *United States v. Runyan,* 275 F.2d 449 (2001).

6. The search LPD conducted pursuant to a search warrant was valid because LPD had probable cause to believe the USB device contained child pornography via the statements made to Officer Paz by the Sames['] employees and the Officers' subsequent confirmatory searches. See [*U*]*s. Const. amend. IV* and *Texas Constitution Article* 1, *section* 9. Officer Paz presented the information to the magistrate through his probable cause affidavit in good faith.

7. The subsequent search warrants were valid because LPD developed probable cause by and through the forensic analysis of the [thumb drive] confirmed that the child pornography within it did not originate from Limon's computer and the [thumb drive] contained personal images of [Salinas]. See *US Const. amend IV* and *Texas Constitution Article* 1, *section 9.*

8. [Salinas] is not entitled to a hearing under *Franks* v. *Delaware* because [Salinas] failed to make a substantial preliminary showing that the affiant, Investigator Charlie Rosales, knowingly or intentionally made false statements, or recklessly disregarded the truth, in his search warrant affidavit. *Franks* v. *Delaware,* 438 U.S. 154 (1978); *Harris* v. *State,* 227 S.W.3d 83, 85 (Tex. Crim. App. 2007).

9. If [Salinas] did establish a violation under *Franks*, the search warrant affidavit still establishes sufficient probable cause because Limon saw what he believed to be pornographic images of underage girls. *Franks,* 438 U.S. at 155; *Harris,* 227 S.W.3d at 85.

Following the denial of his motion, Salinas entered into a plea agreement with the State, pursuant to which: he pleaded guilty to two counts of possession of child pornography; the State dismissed the remaining counts; and his punishment was assessed at ten years' imprisonment in the Texas Department of Criminal Justice Institutional Division for count one and two years' imprisonment for count two, with the sentences running concurrently. The trial court accepted the agreement, and this appeal followed.

II. STANDARD OF REVIEW

In reviewing a trial court's ruling on a motion to suppress, we apply a bifurcated standard of review, giving almost total deference to a trial court's determination of historical facts and mixed questions of law and fact that rely upon the credibility of a witness, but applying a de novo standard of review to pure questions of law and mixed questions that do not depend on credibility determinations. *State v. Martinez*, 570 S.W.3d 278, 281 (Tex. Crim. App. 2019). When a trial judge makes written findings of fact, such as here, we examine the record in the light most favorable to the ruling and uphold those fact findings so long as they are supported by the record. *Baird v. State*, 398 S.W.3d 220, 226 (Tex. Crim. App. 2013). We then proceed to a de novo determination of the legal significance of the facts as found by the trial court. *Id*. We will uphold the trial court's ruling if it is supported by the record and correct under any theory of law applicable to the case. *Young v. State*, 283 S.W.3d 854, 873 (Tex. Crim. App. 2009).

III. SEARCH OF THE THUMB DRIVE

By his first issue, Salinas argues that the trial court should have suppressed the evidence from his thumb drive under the Texas exclusionary rule because (1) he had an expectation of privacy in the thumb drive, and (2) Sames's employees committed a crime when they accessed it. *See* TEX. CODE CRIM. PROC. ANN. art. 38.23(a) ("No evidence obtained by an officer or other person in violation of any . . . laws of the State of Texas . . . shall be admitted in evidence against the accused on the trial of any criminal case."); TEX. PENAL CODE ANN. § 33.02(a) ("A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner."). The State contends that Salinas did not have an

expectation of privacy in the truck and its contents because he turned it over to Sames, and that Sames's employees did not commit a crime when they accessed the thumb drive because the thumb drive is not a "computer" as defined under the relevant statute. *See* TEX. PENAL CODE ANN. § 33.02(a); *see also id.* § 33.01(4) (defining "computer").

The relevant facts are undisputed: Salinas dropped off his truck for service at Sames "for the purpose of testing or inspection"; during service, the technicians working on his truck found a thumb drive in the door compartment; the thumb drive device was unrelated to any of the work performed on the truck by the technicians; the technicians discovered child pornography on the thumb drive and contacted police; and the police came to Sames, viewed the images, and seized the thumb drive.

A. Expectation of Privacy

To prevail on an alleged violation of the Texas exclusionary rule; the Fourth Amendment of the United States Constitution; and article I, § 9 of the Texas Constitution, a defendant must first establish his standing to challenge the admission of the evidence obtained by proof that he had a legitimate expectation of privacy in the place invaded. *See* TEX. CODE CRIM. PROC. ANN. art. 38.23(a); *Matthews v. State*, 431 S.W.3d 596, 606 (Tex. Crim. App. 2014); *Villarreal v. State*, 935 S.W.2d 134, 138 (Tex. Crim. App. 1996); *Kane v. State*, 458 S.W.3d 180, 183–84 (Tex. App.—San Antonio 2015, pet. ref'd). Whether a legitimate expectation of privacy exists is a question of law. *Villarreal*, 935 S.W.2d at 138 n.5. The defendant bears the burden of proving facts establishing a legitimate expectation of privacy. *Id.* at 138. "To carry this burden, the accused must normally prove: (1) that by his conduct, he exhibited an actual subjective expectation of privacy, i.e., a genuine intention to preserve something as private; and (2) that

circumstances existed under which society was prepared to recognize his subjective expectation as reasonable." *Id.* (citing *Smith v. Maryland*, 442 U.S. 735, 740 (1979)).

Here, the place invaded and the item searched was Salinas's thumb drive. As such, we must determine whether he had an expectation of privacy in it and its contents. While we agree with the State that Salinas did not have an expectation of privacy in his truck generally, the question is whether he maintained an expectation of privacy in his thumb drive located in the vehicle. We conclude that Salinas did maintain such an expectation of privacy.

1. Subjective Expectation of Privacy

The subjective prong requires us to determine whether Salinas, "by his conduct, has exhibited an actual expectation of privacy." *See Bond v. United States*, 529 U.S. 334, 338 (2000).

Individuals have a reasonable expectation of privacy in the contents of closed containers and digital storage devices. *See United States v. Ross*, 456 U.S. 798, 822–23 (1982) ("[T]he Fourth Amendment provides protection to the owner of every container that conceals its contents from plain view."); *United States v. Villarreal*, 963 F.2d 770, 773 (5th Cir. 1992) ("The Supreme Court has concluded that 'a constitutional distinction between worthy and unworthy containers would be inappropriate.'" (quoting *Ross*, 456 U.S. at 822)); *see also United States v. Barth*, 26 F. Supp. 2d 929, 936–37 (W.D. Tex. 1998) (finding that the owner of a computer manifested a reasonable expectation of privacy in the contents of data files by storing them on a computer hard drive); *United States v. Reyes*, 922 F. Supp. 818, 832–33 (S.D.N.Y. 1996) (accepting the defendant's assertion that he had a reasonable expectation of privacy in the contents of a pager's memory);

United States v. Blas, No. 90-CR-162, 1990 WL 265179, at *21 (E.D. Wis. Dec. 4, 1990) ("[T]his court finds that an individual has the same expectation of privacy in a pager, computer[,] or other data storage and retrieval device as in a closed container . . . .").

By keeping files in an electronic storage unit—the thumb drive here—Salinas exhibited a subjective expectation of privacy because the thumb drive served as a container that hid its contents from the public. *See Bond*, 529 U.S. at 338; *Ross*, 456 U.S. at 822–23; *Villarreal*, 963 F.2d at 773. Contrary to the State's argument, this subjective expectation of privacy was not diminished by Salinas's leaving of the thumb drive in the truck while it was serviced because the thumb drive was unrelated to any actions needed to service the truck, the inside of the truck was not accessible to the general public or a common area, and Salinas turned the truck over to Sames and its employees solely for the purpose of "testing or inspection." *See United States v. Fultz*, 146 F.3d 1102, 1105 (9th Cir. 1998) ("A person does not forfeit [his] expectation of privacy merely because the container is located in a place that is not controlled by the container's owner."); *Rogers v. State*, 113 S.W.3d 452, 457–58 (Tex. App.—San Antonio 2003, no pet.) (concluding that the defendant had a subjective expectation of privacy in the JPEG files located in his computer's hard drive); *cf. Kane*, 458 S.W.3d at 184–85 (concluding that defendant lacked a subjective expectation of privacy in his flash drive because he left it "in a public computer, in a classroom at Schreiner University[, which was at a minimum] open to other students, faculty, and staff of the University"); *Miller v. State*, 335 S.W.3d 847, 855 (Tex. App.—Austin 2011, no pet.) (concluding that the defendant lacked a subjective expectation of privacy because he "left the thumb drive unattended, unidentified, and unsecured in an area open to his co-workers and other individuals"); *see also Barth*, 26

F. Supp. 2d at 936–37 (concluding that owner of a computer manifested a reasonable expectation of privacy in the contents of data files on the computer's hard drive, despite turning over the computer to a technician for repairs, because he "gave the hard drive to [repairman] for the limited purpose of repairing a problem unrelated to [the] specific files").

We conclude that, under the facts of this case, Salinas had a subjective expectation of privacy in the thumb drive located in his truck.

2. Objectively Reasonable Expectation

To sustain a challenge to the evidence, Salinas's must also show an objectively reasonable expectation of privacy; in other words, it must be an expectation that society is willing to recognize as reasonable. *See Villarreal*, 935 S.W.2d at 138. In determining whether the expectation of privacy is objectively reasonable, courts consider the totality of the circumstances, including: (1) whether the accused had a property or possessory interest in the thing seized or the place invaded; (2) whether the accused was legitimately in the place invaded; (3) whether the accused had complete dominion or control and the right to exclude others; (4) whether, before the intrusion, the accused took normal precautions customarily taken by those seeking privacy; (5) whether the accused put the place to some private use; and (6) whether the accused's claim of privacy is consistent with historical notions of privacy. *Id.* This list is not exhaustive, and no single factor is dispositive of a particular assertion of privacy. *Granados v. State*, 85 S.W.3d 217, 223 (Tex. Crim. App. 2002). Furthermore, these factors are more applicable when discussing the expectation of privacy in a particular physical place rather than in a computer hard drive or even a closed container. *Rogers*, 113 S.W.3d at 457.

Here, Salinas had a property interest in his thumb drive because it belonged to him. Although Salinas was not present when the technicians servicing his vehicle located his thumb drive inside the truck and searched it, this did not diminish his expectation of privacy in the thumb drive to a degree that it became objectively unreasonable under the circumstances of this case. This is because, as testified by Sames's employees, access to the thumb drive was in no way required to complete the tasks for which the truck was given to Sames. *Cf. Lown v. State*, 172 S.W.3d 753, 761 (Tex. App.—Houston [14th Dist.] 2005, no pet.) ("[A]ctions requesting that the [computer] system be backed up and allowing [a third party] to keep copies of the backed up disks are not consistent with historical notions of privacy."); *Rogers*, 113 S.W.3d at 458 (concluding that the defendant did not have a reasonable expectation of privacy in JPEG files on his computer's hard drive because "he expressly directed the computer technician to back up the [JPEG] files"); *see also Barth*, 26 F. Supp. 2d at 936–37 (suppressing evidence because the computer technician did not have authority to open the files unrelated to the repairs he was tasked with as to the computer left with him). In other words, Salinas turned over the truck to Sames for a limited purpose unrelated to the thumb drive, he never consented to the use of the thumb drive, and he did not leave the thumb drive in a place where private parties apart from Sames's employees would come into contact with it. *Cf. Kane*, 458 S.W.3d at 185 (concluding defendant did not have objectively reasonable expectation of privacy in a thumb drive left in a university classroom because "in order to return the drive to [defendant], others must have taken possession of the drive and possibly accessed it to ascertain whether it belonged to" Kane); *Miller*, 335 S.W.3d at 858 (noting that the record supported the denial of the defendant's motion to suppress because, "by leaving

his thumb drive in an area accessible to all of his co-workers, and by allowing them to put the drive in his box if it was found, [defendant] gave effective consent for his co-workers to access the drive in order to identify whether the drive belonged to him").

Furthermore, even though Salinas left the thumb drive in his truck where it was accessible to others during the vehicle's service and did not encrypt its contents or secure them with a password, the limited purpose of the technicians' access to the vehicle and the nature of a thumb drive makes Salinas's claim of privacy consistent with historical notions of privacy. *See United States v. Finley*, 477 F.3d 250, 259 (5th Cir. 2007) (rejecting the government's position that because the cell phone belonged to the employer, the defendant did not have standing to challenge the search of the phone; the defendant had use of phone and took normal precautions to protect privacy of phone calls and records even though he did not have password protection). This is because of the large quantity and type of information that can be stored in a thumb drive, including highly sensitive personal, private, and privileged information. *See United States v. Barber*, 777 F.3d 1303, 1305 (11th Cir. 2015) ("Barber had standing to challenge the search of his bag, even if he lacked standing to contest the search of his car."); *Brackens v. State*, 312 S.W.3d 831, 837 (Tex. App.—Houston [1st Dist.] 2009, pet. ref'd) ("[W]e note that one does not necessarily lose one's reasonable expectation of privacy in one's closed computer files by handing one's computer over to a computer technician."); *Wilson v. State*, 99 S.W.3d 767, 770 (Tex. App.—Houston [14th Dist.] 2003, pet. ref'd) ("A general expectation of privacy in a purse or backpack is reasonable because such baggage is intended as a repository of personal effects."); *see also Fultz*, 146 F.3d at 1105 (noting that "certain types of containers—suitcases, valises, purses, and footlockers, for

instance—do command high expectations of privacy"). Like a cell phone or a purse, a thumb drive is a personal device, and its owner is reasonably entitled to expect that the contents of the drive will remain private. *See State v. Granville*, 423 S.W.3d 399, 405–06 (Tex. Crim. App. 2014) (holding that "(1) a person has a subjective expectation of privacy in the contents of his cell phone, and (2) this expectation of privacy is one that society recognizes as reasonable and legitimate."); *Kelso v. State*, 562 S.W.3d 120, 135 (Tex. App.—Texarkana 2018, pet. ref'd) ("Searching a person's cell phone is like searching his home desk, computer, bank vault, and medicine cabinet all at once.").[7]

The State argues that Salinas did not have an objectively reasonable expectation of privacy because "this particular truck did have a USB-based sound system capable of playing music from [thumb] drives, and the technicians confirmed they expected the drive to contain music."[8] We are not persuaded. As noted in the trial court's findings of fact, Salinas gave permission to Sames "to operate *this vehicle* on any street or road for the purpose of testing or inspection," but the thumb drive is not part of the vehicle and its use is not necessary for the vehicle's operation. Furthermore, the issues Salinas reported with the car—the "check engine" light being on, the air conditioner blowing hot air, and part of the glove compartment being detached—had nothing to do with the thumb drive or the USB-based sound system.

[7] Although a person may have a reasonable and legitimate expectation of privacy in the contents of his thumb drive, he may lose that expectation under some circumstances, such as if he abandons it, lends it to others to use, or gives his consent to its search. *See State v. Granville*, 423 S.W.3d 399, 409, 416 (Tex. Crim. App. 2014). There is no evidence that Salinas did any of this.

[8] Neither Eden nor Limon testified they "expected" to find music in Salinas's thumb drive; rather, Eden stated he looked through the thumb drive out of "curiosity" and because he was "looking for music." Likewise, Limon stated that he and Eden looked through the thumb drive "to see if it had some music on it."

The State also argues that Salinas mislaid or lost the thumb drive. The misplacement or loss of personal property may diminish an individual's expectation of privacy because a party who finds the property may examine and search the property to determine its owner. *See, e.g.*, *Kane*, 458 S.W.3d a 185. However, there are no such facts here undermining Salinas's expectation of privacy because the thumb drive was in his truck, and no third party would have to look through its contents to determine who it belonged to and return it to Salinas. *Cf. Oseguera-Viera v. State*, 592 S.W.3d 960, 965 (Tex. App.—Houston [1st Dist.] 2019, pet ref'd); *Kane*, 458 S.W.3d at 185; *see also United States v. Nealis*, 180 F. Supp. 3d 944, 950 (N.D. Okla. 2016) ("When an individual loses or mislays personal property, his or her 'expectation of privacy is diminished to the extent that the finder may examine and search the lost property to determine its owner." (quoting *State v. Kealey*, 907 P.2d 319, 326 (Wa. 1995))). Thus, even though Salinas told police that he did not "remember" the thumb drive, it was located in his vehicle, and we cannot conclude that this diminished his expectation of privacy.

We conclude that Salinas had an objectively reasonable expectation of privacy in his thumb drive under the facts of this case.

C. Commission of Crime by Mechanics

Because Salinas had both a subjectively and objectively reasonable expectation of privacy in the thumb drive, he had standing to challenge its admission, and we proceed to consider the specific grounds for suppression raised by Salinas. Salinas first argues the evidence from his thumb drive should have been suppressed because Sames's employees committed a crime when they accessed it, and thus, admission of the evidence violates the Texas exclusionary rule.

The Texas exclusionary rule provides that "[n]o evidence obtained by an officer or other person in violation of any . . . laws of the State of Texas . . . shall be admitted in evidence against the accused on the trial of any criminal case." TEX. CODE CRIM. PROC. ANN. art. 38.23(a); *Miles v. State*, 241 S.W.3d 28, 36 (Tex. Crim. App. 2007). In Texas, it is a crime to knowingly access "a computer, computer network, or computer system without the effective consent of the owner." TEX. PENAL CODE ANN. § 33.02(a). A "computer" is defined as "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device that performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses and includes all input, output, processing, storage, or communication facilities that are connected or related to the device." *Id.* § 33.01(4).

Salinas argues that his thumb drive is a "computer" under the statutory definition; the State argues it is not. The trial court concluded that the thumb drive was not a "computer" for purposes of § 33.02 of the penal code. This is a legal conclusion we review de novo. *See Baird*, 398 S.W.3d at 226.

The penal code does not define "data processing." When a statutory term is not defined, we attempt to give effect to its plain meaning or common understanding. *See Ramos v. State*, 303 S.W.3d 302, 306 (Tex. Crim. App. 2009); *Boykin v. State*, 818 S.W.2d 782, 785 (Tex. Crim. App. 1991). In doing so, we may consult standard dictionaries. *Ramos*, 303 S.W.3d at 306. Webster's dictionary defines "data processing" as "the converting of raw data to machine-readable form and its subsequent processing (such as storing, updating, rearranging, or printing out) by a computer." MERRIAM-WEBSTER'S ONLINE DICTIONARY, https://www.merriam-webster.com/dictionary/data-

processing (last visited Apr. 14, 2021); *see Data Processing*, ENCYCLOPEDIA BRITANNICA, https://www.britannica.com/technology/data-processing (last visited Apr. 22, 2021) (defining "Data Processing" as "Manipulation of data by a computer. It includes the conversion of raw data to machine-readable form, flow of data through the CPU and memory to output devices, and formatting or transformation of output"). A thumb drive stores data in memory cells, but it does not "convert[] raw data to machine-readable form" or otherwise perform "data processing." *See SanDisk Corp. v. Kingston Tech. Co.*, 695 F.3d 1348, 1351 (Fed. Cir. 2012) ("A typical flash memory device includes one or more flash memory integrated circuit chips and a controller. Each flash memory chip contains memory cells for storing data. The cells are arranged as 'pages' with multiple 'pages' comprising a 'block' of cells."); *flash drive*, MERRIAM-WEBSTER'S ONLINE DICTIONARY, https://www.merriam-webster.com/dictionary/flash-drive (last visited Apr. 14, 2021) (defining "flash drive" or "thumb drive" as "a data storage device that uses flash memory[;] specifically: a small rectangular device that is designed to be plugged directly into a USB port on a computer and is often used for transferring files from one computer to another"); MERRIAM-WEBSTER'S ONLINE DICTIONARY, https://www.merriam-webster.com/dictionary/thumb-drive (last visited Apr. 14, 2021) (defining "thumb drive" or "flash drive" as "a small usually rectangular device used for storing and transferring computer data").

Salinas argues that the thumb drive is a computer because the statute defines "computer" as including "all input, output, processing, storage, or communication facilities *that are connected or related to the device*." *See* TEX. PENAL CODE ANN. § 33.01(4). For Salinas's thumb drive to have been a "computer," however, it must have been "connected

or related to" a device that qualified as an "electronic, magnetic, optical, electrochemical, or other high-speed data processing device that performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses . . . ." *See id.* There was no additional device here meeting this definition, and Salinas does not argue that the thumb drive was related to any specific device.

We reject Salinas's arguments and conclude that the thumb drive here is not a "computer" for purposes of § 33.02(a). *See id.* §§ 33.02(a), 33.01(4). As a result, Sames's employees did not commit a crime when they accessed it, and the Texas exclusionary rule is not implicated. *See* TEX. CODE CRIM. PROC. ANN. art. 38.23(a).

D. Unreasonable Search by Police

As the final argument under his first issue, Salinas argues that the evidence should be excluded because law enforcement conducted an unreasonable warrantless search of his thumb drive, violating the Fourth Amendment of the United States Constitution. *See* U.S. CONST. amend IV; TEX. CODE CRIM. PROC. ANN. art. 38.23(a)**.** As a result, Salinas argues, the evidence should be excluded under the exclusionary rule. By his second issue, Salinas argues the trial court should have suppressed the evidence because the Fourth Amendment of the United States Constitution and the Texas Constitution were violated.

The purpose of both the Fourth Amendment and Article I, § 9 of the Texas Constitution is to safeguard an individual's legitimate expectation of privacy from unreasonable governmental intrusions. *Rogers*, 113 S.W.3d at 456–57; *see* U.S. CONST. amend. IV; TEX. CONST. art. I, § 9. A warrantless search is considered per se unreasonable subject to a few specifically defined and well-established exceptions.

McGee v. State, 105 S.W.3d 609, 615 (Tex. Crim. App. 2003). One such exception is the private search doctrine. *See United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (noting that the Fourth Amendment "is wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as the agent of the Government or with the participation or knowledge of any government official"); *State v. Rodriguez*, 521 S.W.3d 1, 10–11 (Tex. Crim. App. 2017). Under the private search doctrine, the government does not conduct a Fourth Amendment search when there is a "virtual certainty" that its search will disclose nothing more than what a private party's earlier search has revealed. *Jacobsen*, 466 U.S. at 119; *see Burdeau v. McDowell*, 256 U.S. 465, 475 (1921); *United States v. Reddick*, 900 F.3d 636, 637–39 (5th Cir. 2018) ("Under the private search doctrine, 'the critical inquiry under the Fourth Amendment is whether the authorities obtained information with respect to which the defendant's expectation of privacy has not already been frustrated." (quoting *United States v. Runyan*, 275 F.3d 449, 461 (5th Cir. 2001))). In other words, once a private individual, acting of his own accord, conducts a search—even one that frustrates a defendant's reasonable expectation of privacy—the Fourth Amendment does not forbid law enforcement from replicating the search to confirm its findings, as long as law enforcement officials constrain their search to the parameters of the search conducted by the private individual. *See Jacobsen*, 466 U.S. at 117–18, 126; *Reddick*, 900 F.3d at 637–39; *Rodriguez*, 521 S.W.3d at 11 ("In [private search doctrine] cases the police make no search at all as the property is seized by a private party without any intrusion on an expectation of privacy by law enforcement."); *see also Illinois v. Andreas*, 463 U.S. 765, 769 n.2 (1983) ("When common carriers discover contraband in packages entrusted to their care, it is routine for

them to notify the appropriate authorities. The arrival of police on the scene to confirm the presence of contraband and to determine what to do with it does not convert the private search by the carrier into a government search subject to the Fourth Amendment."); *United States v. Rivera-Morales*, 961 F.3d 1, 4 (1st Cir. 2020) ("In general terms, [the private search] doctrine provides that law enforcement officers may, without a warrant, examine evidence that a private party has unearthed and made available to them, as long as their actions remain within the scope of the antecedent private search.").

Here, the trial court found that the thumb drive had two folders, one of which was titled "ZZZZ." The trial court further found that all seven images of child pornography were contained in the "ZZZZ" folder and that the thumbnail images would be visible when that folder was opened. These findings are supported by the testimony of the State's forensic expert, Jeff Williams. The trial court also found that Limon accessed the "ZZZZ" folder and observed multiple images, which was supported by the testimony of multiple witnesses. Williams testified that his forensic analysis "indicate[d] that the thumbnail images were viewed [by Sames's employees, because in] order for a thumbnail image to be on [Limon's] computer, that means the image did need to appear in the File Explorer viewing" when they accessed the "ZZZZ" folder. As a result, Sames's employees frustrated Salinas's expectation of privacy in all of the illegal images in the thumb drive. Therefore, there was no Fourth Amendment violation when the officers later searched the thumb drive and viewed the images. *See Jacobsen*, 466 U.S. at 117 ("Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-nonprivate information.").

Salinas points to the testimony of his own forensic examiner that there was considerably more activity with regards to clicking through multiple files when the police searched the drive. Officer Paz testified that he clicked through the images in the "ZZZZ" folder, and the Sames employees testified that they did not. As noted above, Williams explained that Limon and Eden would have seen thumbnails of all seven images once the "ZZZZ" folder was opened. Even if they never clicked on the thumbnails or viewed the full-size images, the employees saw enough to know that what they were viewing was illegal and should be reported to police. Thus, Salinas's expectation of privacy was already frustrated, regardless of whether law enforcement officers later clicked on each image to open them individually. *See id.* at 117–18, 126; *Reddick*, 900 F.3d at 637–39.

We conclude that the private search doctrine applies here, and therefore, law enforcement did not violate the Fourth Amendment of the United States Constitution or Article I, § 9 of the Texas Constitution when they viewed the images, and the evidence does not violate the Texas exclusionary rule. *See Jacobsen*, 466 U.S. at 117; *Walter v. United States*, 447 U.S. 649, 657 (1980); *Reddick*, 900 F.3d at 639 (concluding there was no separate search triggering the Fourth Amendment when investigator opened files sent by Microsoft that Microsoft had identified as child pornography when they were uploaded by Reddick); *see also United States v. Harling*, 705 Fed. App'x 911, 916 (11th Cir. 2017) (per curiam) ("[L]aw enforcement's subsequent search of the first and second USB drives, after listening to Nicole and Ada describe in detail what they had observed, was not violative of the Fourth Amendment [because] it did not meaningfully exceed the scope of Ada's search."); *United States v. Tosti*, 733 F.3d 816, 822 (9th Cir. 2013) ("Even assuming that Detective Shikore viewed enlarged versions of the thumbnails, he still did not exceed

the scope of Suzuki's prior search because Suzuki and both detectives both testified that they could tell from viewing the thumbnails that the images contained child pornography.").[9]

E. Conclusion

Salinas's first and second issues are overruled.

IV. *FRANKS* HEARING

By his third issue, Salinas argues the trial court abused its discretion when it concluded that (1) he was not entitled to a *Franks* hearing, and (2) even if there had been a *Franks* violation in the affidavit supporting the search warrant, the other untainted facts in the affidavit would still be sufficient to support probable cause.

> [W]here the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the alleged false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request. In the event that at that hearing the allegation of perjury or reckless disregard is established by the defendant by a preponderance of the evidence, and, with the affidavit's false material set to one side, the affidavit's remaining content is insufficient to establish probable cause, the search warrant must be voided and the fruits of the search excluded to the same extent as if probable cause was lacking on the face of the affidavit.

Franks v. Delaware, 438 U.S. 154, 155–56 (1978); *see Cates v. State*, 120 S.W.3d 352, 355 (Tex. Crim. App. 2003).

Salinas argues that the affidavit in support of the warrant here contained a false statement because it claimed that "Luna . . . and his co-workers accessed the [thumb

[9] Salinas also argues that Sames's employees were not capable of consenting to the search of the thumb drive by police. Voluntary consent is another exception to the Fourth Amendment warrant requirement. *See State v. Rodriguez*, 521 S.W.3d 1, 11 (Tex. Crim. App. 2017); *Valtierra v. State*, 310 S.W.3d 442, 448 (Tex. Crim. App. 2010). Having concluded that the private search doctrine exception to the warrant requirement applies here, we do not need to address this argument. *See* TEX. R. APP. P. 47.1.

drive] to check whether the USB port in Dr. Salinas's vehicle was operating properly," and thus, the affidavit "told the magistrate . . . that the initial accessing of the [thumb drive] was done with Dr. Salinas's consent." As noted above, Sames's employees lied when they told law enforcement that use of the thumb drive was part for any of the work they performed on Salinas's truck. The search warrant affidavit contained this false information. However, for a violation of *Franks*, the false statements must be made by the affiant himself, not by a third party. *Franks*, 438 U.S. at 155–56, 164–65 (noting that the Fourth Amendment requires the probable cause affidavit to make a truthful showing "in the sense that the information put forth is believed or appropriately accepted by the affiant as true"); *see Hackleman v. State*, 919 S.W.2d 440, 448 (Tex. App.—Austin 1996, pet. ref'd untimely filed); *see also McCray v. Illinois*, 386 U.S. 300, 307 (1967) (explaining that when determining whether probable cause exists to support a search warrant, "the magistrate is concerned, not with whether the informant lied, but with whether the affiant is truthful in his recitation of what he was told"); *United States v. Johnson*, 580 F.3d 666, 670 (7th Cir. 2009) ("It is not enough to show that an informant lied to the government officer, who then included those lies in the complaint. Instead, the evidence must show that the officer submitting the complaint perjured himself or acted recklessly because he seriously doubted or had obvious reasons to doubt the allegations."). Thus, to qualify for a *Franks* hearing, Salinas needed to make a substantial showing that Investigator Rosales knew of the falsity of the statements, or recklessly disregarded the truth. Salinas failed to do so. And the trial court's finding that Officer Paz had no cause to disbelieve the false report given by Luna is supported by the record. *See Baird*, 398 S.W.3d at 226.

Salinas's third issue is overruled.

V. CONCLUSION

The trial court's judgments of conviction are affirmed.

DORI CONTRERAS
Chief Justice

Publish.
TEX. R. APP. P. 47.2(b).

Delivered and filed on the
13th day of May, 2021.