No. _____

In the Supreme Court of the United States

JASON WILLIAM DOBBS,

Petitioner,

v.

THE STATE OF NEVADA,

Respondent.

ON PETITION FOR A WRIT OF CERTIORARI
TO THE SUPREME COURT OF NEVADA

PETITION FOR A WRIT OF CERTIORARI

Thomas L. Qualls
Counsel of Record
WASHOE COUNTY ALTERNATE PUBLIC DEFENDER
350 South Center Street, 6th Floor
Reno, Nevada 89501
(775) 328-3955
TLQualls@washoecounty.gov

Attorney for Petitioner

United States Commercial Printing Company • www.uscpc.us • (202) 866-8558 • print@uscpc.us • Appellate Legal Printer

QUESTIONS PRESENTED

1. Whether the Fourth Amendment requires law enforcement to make *sufficient inquiries* as to the authority of a third person to consent to a warrantless search of a computer hard drive.

2. Whether state courts must employ the *sufficient inquiry* test when reviewing a Fourth Amendment challenge to a warrantless search of a computer hard drive based upon the apparent authority of a third person.

RELATED PROCEEDINGS

Nevada Supreme Court (panel):

Dobbs v. State, No. 89954, 573 P.3d 1248 (August 14, 2025) (unpublished)(*Order of Affirmance*)

Dobbs v. State, No. 89954, (September 15, 2025) (*Order Denying Rehearing*)

Nevada Supreme Court (*en banc*):

Dobbs v. State, No. 89954, (October 02, 2025) (en banc reconsideration denied)

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

PETITION FOR A WRIT OF CERTIORARI

Petitioner Jason William Dobbs respectfully petitions for a writ of certiorari to the Nevada Supreme Court in *Dobbs* v. *State*, No. 89954.

OPINIONS BELOW

The opinion of the Nevada Supreme Court in *Dobbs* v. *State*, Case No. 89954, is reported at 573 P.3d 1248 (Nev. 2025) and appears in the Appendix as Appendix A.

JURISDICTION

The opinion of the Nevada Supreme Court was filed on August 14, 2025. The same panel of the court denied Petitioner's timely petition for rehearing on September 15, 2025. The en banc court denied reconsideration on October 2, 2025. This Court has jurisdiction under 28 U.S.C. § 1257(a).

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

The Fourth Amendment to the U.S. Constitution provides: "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, and particularly describing the place to be searched, and the persons or things to be seized."

STATEMENT OF THE CASE

Law enforcement officials in Nevada conducted a warrantless search of a computer hard drive belonging to Petitioner Jason William Dobbs, without making sufficient inquiries into whether the person who consented to the search of the hard drive had authority to consent to the search. Petitioner seeks review of the state court ruling which failed to employ the proper legal test regarding apparent authority to consent to a warrantless search.

1. The Fourth Amendment prohibits warrantless searches of a person's home or possessions. *Illinois* v. *Rodriguez*, 497 U.S. 177 (1990). With few exceptions, the question whether a warrantless search is reasonable and hence constitutional must be answered no. *Kyllo* v. *United States*, 533 U.S. 27, 31 (2001). A person has an expectation of privacy in his or her private, closed containers. *United States* v. *Davis,* 332 F.3d 1163, 1167 (CA9 2003).

Third-party consent is determined by "mutual use of the property by persons generally having joint access or control for most purposes ..." over the quarters or objects to be searched. *United States* v. *Matlock,* 415 U.S. 164, 171, n. 7 (1974); *Illinois* v. *Rodriguez,* 497 U.S. 177, 177 (1990). If the party giving consent to the search is not the target of an investigation, that person must reasonably be believed by law enforcement to have lawful access and control over the item to be searched. *Matlock*, 415 U.S. at 171 n. 7.

When a defendant clearly manifests an expectation of privacy by locking a container and does not provide any suggestion of a right of general access or mutual use of the property, a third party does not have actual authority to consent to the search. *United States* v. *Barry*, 853 F.2d 1479, 1482 (CA8 1988).

The Ninth Circuit has ruled that if law enforcement conducts a search based on third-party consent in a state of near ignorance, without obtaining sufficient information about that party's authority, the Court *cannot* conclude that there was an objectively reasonable belief that the third party had authority to consent to a search. *United States* v. *Arreguin*, 735 F.3d 1168, 1175 (CA9 2013). Similarly, the Ninth Circuit has held that the "mere fact of access, without more, does not indicate that the access was authorized." *United States* v. *Reid*, 226 F.3d 1020, 1025 (CA9 2000).

2. Petitioner worked in the information technology ("IT") field. He was the Director of IT for a medical imaging company in Sparks, Nevada. He was in a romantic relationship with Jayme Hubbard, who had three children from a prior marriage. Petitioner and Hubbard also had two children together. They all lived together. Petitioner and Hubbard were both on the lease of the house they rented, but Dobbs paid the rent and all the bills.

Petitioner's home office was in an open area in their house, and contained a desk and computers and office supplies. The computer at issue in this case was a Windows-based PC and belonged solely to Petitioner. Petitioner's computer was not accessed

by the family. Hubbard had her own Mac computer, and each of the children had their own devices. Hubbard was not familiar with Windows systems, and she knew Petitioner kept a password on his computer, but she did not know what it was.

For various reasons, Hubbard became suspicious that petitioner had taken inappropriate pictures of her daughters, including on one occasion when two of the girls were in the shower together. While petitioner was away on a camping trip, Hubbard took the hard drive from petitioner's computer and brought it to Lieutenant Cox, who was the head of the Washoe County Sheriff's Internet Crimes Against Children Unit.

She explained to Cox that she had access to the office space where the devices were kept, but that the devices belonged to Petitioner. She testified that she told Cox that though she had access to the office space, she "didn't have access to whatever was on the devices." She told Cox that the hard drive and computer belonged to petitioner.

Lt. Cox took possession of the hard drive. Hubbard read and signed a Consent to Search form in his presence. There is a section above the signature that reads, "*Please list any passwords to devices*." Hubbard left that section blank on the form. Cox testified he did not ask her to fill that in that information. He also testified that he did not inquire as to why that was left blank. Cox further testified that he did not ask Hubbard about whether the hard drive was password-protected. Nor did he attempt to log in to the drive to see if anything on it was password protected.

Lt. Cox was aware that the computers belonged to petitioner. He knew Dobbs was the primary user of the computer. And he had no knowledge of how Hubbard used the office space. Cox explained that he did not ask for that information nor make any further inquiries about passwords, because, "with these devices passwords aren't important to the forensic examination of each device. Devices can be -- there's a different variety of ways to get into them that can be used."

Lt. Cox testified he did not ask Hubbard if she had her own computer or if the kids had their own computer. He admitted Hubbard did not say if she had looked at what was on the device. He admits that he did not ask her if she had looked at the device. Rather than ask these questions about ownership, access, use, and viewing, Lt. Cox made the assumption "[t]hat she didn't want to see what might be on there herself." He admitted that he did not ask any follow up questions or do anything to assure that his assumption was correct.

Lt. Cox then took the hard drive to Detective Harris with the Sparks Police Department. Harris imaged the hard drive and found some child sexual abuse material (CSAM) on the drive. Harris explained that the hard drive showed only one user account, for petitioner, which was password protected. There was not an account on the hard drive for Hubbard.

3. After the imaging of the hard drive, Petitioner was charged with several CSAM offenses. He filed a *Motion to Suppress Evidence Obtained During an Illegal Search*, based upon Lt. Cox's lack of sufficient inquiry into whether Hubbard had authority

to consent to the warrantless search. A two-day hearing was held on the matter on September 18-19, 2024. Following the hearing, on October 23, 2024, the district court entered an *Order Denying Motion to Suppress Evidence Obtained During an Illegal Search*.

The parties then negotiated a conditional plea, expressly allowing Dobbs to raise the suppression issue on appeal. Dobbs entered guilty pleas on all counts pursuant to the conditional plea agreement. Then he filed a timely appeal to the Nevada Supreme Court.

4. On August 14, 2025, a Nevada Supreme Court panel of three justices affirmed petitioner's conviction, omitting in its opinion any discussion of the sufficient inquiry test regarding third-party consent or any reference to controlling authorities on the matter. Petitioner filed a timely petition for rehearing to the panel on August 22, 2205. The panel denied the petition for rehearing on September 15, 2025, without analysis. Petitioner then filed a petition for *en banc* reconsideration to the full Nevada Supreme Court on September 15, 2025. The *en banc* court denied reconsideration on October 2, 2025, also without any analysis. The instant Petition for Writ of Certiorari follows.

REASONS FOR GRANTING THE PETITION

The Fourth Amendment protects against *unreasonable* warrantless searches. *Rodriguez*, 497 U.S. at 185. In assessing the reasonableness of a search, this Court

has held that, "the rights protected by the Fourth Amendment are not to be eroded ... by unrealistic doctrines of 'apparent authority.'" *Stoner* v. *California,* 376 U.S. 483, 488 (1964).

In *Rodriguez*, this Court concluded that the test for reasonableness of a search pursuant to a third-party consent is an objective one: "[W]ould the facts available to the officer at the moment ... 'warrant a man of reasonable caution in the belief' " that the consenting party had authority over the premises? … If not, then warrantless entry without further inquiry is unlawful unless authority actually exists." *Rodriguez*, 497 U.S. at 188–89, quoting *Terry* v. *Ohio,* 392 U.S. 1, 21–22 (1968).

When the property to be searched is a container (as a computer hard drive is), the inquiry must examine the third party's relationship to that container, *Matlock,* 415 U.S. at 171 & n. 7 (1974). Further, the inquiry must include whether circumstances indicate that the third party lacks access to the contents of the container. *United States* v. *Fultz,* 146 F.3d 1102, 1106 (CA9. 1998).

As noted in *Rodriguez*, even when a third-party asserts that they have authority to consent, law enforcement may not conduct a warrantless search upon that assertion, alone:

> Even when the invitation is accompanied by an explicit assertion that the person lives there, the surrounding circumstances could conceivably be such that a reasonable person would doubt its truth and not act upon it without further inquiry.

Rodriguez, 497 U.S. at 188

Petitioner asks that the Court affirmatively clarify that the rule in *Rodriguez* applies to invitations to search password-protected computers, just as it does to invitations to search premises. Specifically, Dobbs asks that this Court clarify that *sufficeint inquiry* regarding an invitation to search a computer must include whether the computer is jointly used and whether the user who is not present has their files protected by password.

As clearly articulated by this Court in *Rodriguez* and the Ninth Circuit in *United States* v. *Arreguin, infra*, law enforcement officers cannot use the apparent authority doctrine to justify a warrantless search when they fail to make sufficient inquiry into the third party's authority to consent to a warrantless search.

I. This Court Should Grant Review to Clarify that Law Enforcement Must Make Sufficient Inquiry Into a Third Person's Authority to Consent to a Warrantless Search of a Computer Device.

A. The Nevada Supreme Court's Decision, Which Omits the *Sufficient Inquiry* Test, Contravenes This Court's Precedent and the Precedent of Several United States Courts of Appeals, Including the Ninth Circuit.

The protections of the Fourth Amendment are not mere "formalities." As this Court articulated in *McDonald* v. *United States*, 335 U.S. 451 (1948):

> We are not dealing with formalities. The presence of a search warrant serves a high function... The right of privacy was deemed too precious to entrust to the discretion of those whose job is the detection of crime and the arrest of criminals. * * * And so the Constitution requires a magistrate to pass on the desires of the police before they violate the privacy of the

> home. We cannot be true to that constitutional requirement and excuse the absence of a search warrant without a showing by those who seek exemption from the constitutional mandate that the exigencies of the situation made that course imperative.'

Id. at 455-456.

As noted, the Ninth Circuit requires law enforcement to make sufficient inquiry into a third-party's authority to consent to a search, when there is any ambiguity. The Ninth Circuit has expressly prohibited warrantless searches based upon third-party consent, where law enforcement proceeded with the search under a "state of near ignorance." *Arreguin*, 735 F.3d at 1175. See also *Reid*, 226 F.3d at 1025.

Closed containers are treated differently by this Court for Fourth Amendment purposes. Even a valid consent to search a house "may not be effective consent to a search of a closed object inside the home." *United States* v. *Karo*, 468 U.S. 705, 725 (1984). Password-protected files have been compared to a "locked footlocker inside the bedroom." *Trulock* v. *Freeh,* 275 F.3d 391, 403 (CA4 2001).

The Seventh Circuit has recognized that a third-party's authority to consent to a search of a computer depends on "whether they enjoyed mutual use of, access to, and control over the computer itself." *United States* v. *Wright*, 838 F.3d 880, 885 (CA7 2016). "The key to consent is actual or apparent authority *over the area to be searched*." *United States* v. *Basinski*, 226 F.3d 829, 834 (CA7 2000) (emphasis added).

The Fourth Circuit has ruled that where two people both used a computer, and each had joint access to the hard drive, but where the first party protected his

personal files with passwords, the second party did not have authority to consent to a search of the first party's password-protected files. *Trulock*, 275 F.3d at 403.

In examining the issue of third-party consent to search a computer, other courts have looked to the officers' knowledge of whether there was password protection to conclude whether the computer was "locked" in the way as a suitcase or footlocker. In *United States* v. *Morgan,* for example, the Sixth Circuit viewed a wife's statement to police that she and her husband did not have individual usernames or passwords as a factor weighing in favor of the wife's apparent authority to consent to a search of the husband's computer. 435 F.3d 660, 663 (CA6 2006).

See also *United States* v. *Buckner,* 473 F.3d 551, 555–56 (CA4 2007), in which third-party consent was upheld because the consenting wife leased the computer in her name, occasionally used the computer, and fraudulent activity was conducted from the computer using accounts in the wife's name. In *Morgan,* 435 F.3d at 663–64, the court concluded that the third-party consenting wife had apparent authority, because the computer was located in common area of the house, she told police that she used the computer, she and her husband did not have separate usernames or passwords, and she had installed software on the computer. Conversely, where the third party admitted she had no access to or control over the computer or a portion of the computer's files, even when the computer was located in a common area of the house, the court did not find third party authority. *Trulock,* 275 F.3d at 403.

B. There is a Split of Authority Among the Federal Circuit Courts Regarding the Amount of Inquiry Required by Law Enforcement in Apparent Authority Consent Cases.

Unlike the decisions cited herein from the Fourth, Sixth, Seventh, and Ninth Circuits, the Tenth Circuit upheld third-party consent for a warrantless search of a computer, under the apparent authority doctrine, even though law enforcement did not sufficiently inquire into the third-party's access to the computer files. The Court reasoned that the "circumstances reasonably indicated" that the third party had "mutual use of or control over" the computer, and that "the officers were under no obligation to ask clarifying questions." *United States* v. *Andrus*, 483 F.3d 711, 720 (CA10 2007), *decision clarified on denial of reh'g*, 499 F.3d 1162 (CA10 2007).

The *Andrus* Court reached this conclusion, even though it acknowledged that, "[b]ecause intimate information is commonly stored on computers, it seems natural that computers should fall into the same category as suitcases, footlockers, or other personal items that 'command[ ] a high degree of privacy.'" *Andrus*, 483 F.3d at 718, *quoting United States* v. *Salinas–Cano,* 959 F.2d 861, 864 (CA10 1992).

The *Andrus* decision, which did not require law enforcement to make reasonably sufficient inquiry in the third party's authority to consent to the search, has been widely criticized in law review articles and by a prominent legal treatise. See 4 Wayne R. LaFave, *Search and Seizure: A Treatise on the Fourth Amendment* § 8.3(g) at 180 (4th ed.2004, 2010–11 Supplement) ("Remarkably, the majority in *Andrus,* on these

facts, upheld the search on an apparent authority basis."); David D. Thomas, Note, *Dangerously Sidestepping the Fourth Amendment: How Courts Are Allowing Third–Party Consent To Bypass Warrants for Searching Password–Protected Computers,* 57 Clev. St. L.Rev. 279, 304–05 (2009) (It is constitutionally wrong to "allow police officers to skate around the Fourth Amendment by intentionally avoiding asking questions of third parties while obtaining consent, as well as allowing them to ignore password "locks" on computers that, as shown, courts have held to be analogous to locks on physical items."); Michael J. Ticcioni, Comment, *United States v. Andrus: Does the Apparent Authority Doctrine Allow Circumvention of Fourth Amendment Protection in the Warrantless Search of a Password–Protected Computer,* 43 New Eng. L.Rev. 339, 355 (Winter 2009) ("The Tenth Circuit erred in its holding that law enforcement agents were reasonable in relying on the apparent authority of a ninety-one year old man to consent to a search of his son's password-protected computer."); Michael Smith, Survey, *The Fourth Amendment, Password Protected Computer Files and Third Party Consent Searches: The Tenth Circuit Broadens the Scope of Warrantless Searches,* 85 Denv. U.L. Rev 701, 723 (2008) ("The *Andrus* rule essentially does three things: first, it removes the requirement for a third party consenter to have a key to a locked container; second, it replaces the key requirement with a government actor's reasonable belief that there is no need for a key; and third, it allows the use of technology to bypass a key (or password) without first determining whether the container (or computer) is locked."); Noah Stacy, Comments and

Casenotes, *Apparent Third Party Authority and Computers: Ignorance of the Lock is No Excuse,* 76 U. Cin. L.Rev. 1431 (Summer 2008) ("The court's holding sets a dangerous precedent under which law enforcement may evade the Fourth Amendment requirement of either a warrant or valid consent by claiming ignorance of any password protection and relying upon the apparent authority of a third party."); Sarah M. Knight, Casenote, *United States v. Andrus: Password Protect Your Roommate, Not Your Computer,* 26 J. Marshall J. Computer & Info. L. 183, 184 (Fall 2008) ("As a consequence of this holding, third-parties can consent to searches beyond their authority, and individuals' efforts to secure their data are rendered useless.")

C. This Court Should Resolve the Question Presented Here and Now Because More than Ever, Computers and Computer Devices Are Ubiquitous to Our Modern Lives, and They Contain More Constitutionally Protected Information Than Ever.

Computers and computer devices of all kinds are seamlessly integrated into all aspects of our modern lives. Consequently, these devices contain more and more private information about us that is entitled to constitutional protection under the Fourth Amendment's doctrine of the expectation of privacy.

Multiple jurisdictions have already recognized that using a password to protect one's files on a computer creates a reasonable expectation of privacy, similar to any locked container. See, e.g., *Buckner*, 473 F.3d at 554 n.2, in which the court recognized a reasonable expectation of privacy in password-protected computer files. See also

United States v. *Thomas*, 818 F.3d 1230, 1241-42 (CA11 2016), in which the Eleventh Circuit concluded that that by *not* password protecting his files, a defendant "assumed the risk" that the third party could consent to a search of the contents of the computer.

Since the existence of a password is pivotal in these findings, this Court should resolve the question presented, which is that in order for the State to show that a third-party had apparent authority to consent to a warrantless search of the password-protected files, law enforcement must make further inquiry into the following clarifying factors: (1) whether the computer and/or files are password protected; and (2) whether the third-party knows the password; and (3) whether the third-party has mutual use of the computer; and (4) whether the third-party has permission to access the files in question.

The Tenth Circuit's decision in *United States* v. *Andrus* sets a reckless precedent that allows law enforcement to circumvent the Fourth Amendment by simply not asking the right questions. The Nevada Supreme Court's decision in *Dobbs* v. *State* reached the same conclusion as the Tenth Circuit in *Andrus*, by ignoring the requirement that law enforcement make reasonable and sufficient inquiries when faced with a situation of apparent authority to consent to a warrantless search of a computer.

CONCLUSION

The Nevada Supreme Court's Decision in *Dobbs* v. *State*, 573 P.3d 1248 (Nev. 2025), omits the *sufficient inquiry* test that is required in cases involving third-party apparent authority to consent to a warrantless search. The *Dobbs* decision contravenes this Court's precedent and the precedent of several federal circuits, including the Ninth Circuit. Moreover, the Dobbs decision aligns with the Tenth Circuit's decision in *United States* v. *Andrus*, and underscores the split in authority among state and federal courts on this issue. Accordingly, this Court should grant certiorari.

Respectfully submitted,
Thomas L. Qualls
Counsel of Record
WASHOE COUNTY ALTERNATE PUBLIC DEFENDER
350 South Center Street
Reno, Nevada 89501
(775) 328-3955

December 2025