PUBLISHED

UNITED STATES COURT OF APPEALS

FOR THE FOURTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff-Appellee,

v.

FRANK GARY BUCKNER,
Defendant-Appellant.

No. 06-4399

Appeal from the United States District Court
for the Western District of Virginia, at Harrisonburg.
Samuel G. Wilson, District Judge.
(5:05-cr-00006)

Argued: November 29, 2006

Decided: January 11, 2007

Before WIDENER, NIEMEYER, and MOTZ, Circuit Judges.

Affirmed by published opinion. Judge Motz wrote the opinion, in which Judge Widener and Judge Niemeyer joined.

COUNSEL

ARGUED: William Kent Bowers, Harrisonburg, Virginia, for Appellant. Joseph William Hooge Mott, Assistant United States Attorney, OFFICE OF THE UNITED STATES ATTORNEY, Roanoke, Virginia, for Appellee. **ON BRIEF:** John L. Brownlee, United States Attorney, Ashley Nicole Reynolds, Third Year Practice Student, OFFICE OF THE UNITED STATES ATTORNEY, Roanoke, Virginia, for Appellee.

OPINION

DIANA GRIBBON MOTZ, Circuit Judge:

Frank Gary Buckner appeals from an order denying his motion to suppress evidence gathered from password-protected files on the hard drive of a computer police seized from his home. The officers seized and searched the computer, without a warrant, on the basis of oral consent granted by Buckner's wife, Michelle. On appeal, Buckner contends that although Michelle's consent sufficed to give the officers permission to search the computer itself, her consent could not extend to his password-protected files. Because Michelle Buckner did have apparent authority to consent to the search of these files, we affirm.

I.

This criminal investigation began when the Grottoes, Virginia police department received a series of complaints regarding online fraud committed by someone using AOL and eBay accounts opened in the name Michelle Buckner. On July 28, 2003, police officers went to the Buckner residence to speak with Michelle, but only Frank Buckner was at home. The officers then left, asking Frank to have Michelle contact them. A short while later, Frank Buckner himself called the police, seeking more information about why they wanted to speak with Michelle. The police responded that they wanted to talk with her about some computer transactions. That evening, Michelle Buckner went to the police station and told officers that she knew nothing about any illegal eBay transactions, but that she did have a home computer leased in her name. She further stated that she only used the home computer occasionally to play solitaire.

The next day, July 29, police returned to the Buckner residence to speak further with Michelle about the online fraud. Frank Buckner was not present. Michelle again cooperated fully, telling the officers "to take whatever [they] needed" and that she "want[ed] to be as cooperative as she could be." The computer Michelle had indicated was leased in her name was located on a table in the living room, just inside the front door of the residence. Pursuant to Michelle's oral consent, the officers seized the leased home computer.

At the time the officers seized the computer, it was turned on and running, with the screen visibly lit. The officers did not, at this time, open any files or look at any information on the computer. Instead, with Michelle's blessing, they shut down the computer and took its data-storage components for later forensic analysis. This analysis consisted of "mirroring" — that is, creating a copy of — the hard drive and looking at the computer's files on the mirrored copy.

Ultimately, a grand jury indicted Frank Buckner on twenty counts of wire fraud, *see* 18 U.S.C. § 1343 (2000), and twelve counts of mail fraud, *see* 18 U.S.C. § 1341 (2000). At a suppression hearing, Frank Buckner offered the only affirmative evidence on the password issue, testifying that a password was required to use the computer. Buckner stated that he was the only person who could sign on to the computer and the only person who knew the password necessary to view files that he had created. Nothing in the record contradicts this testimony. Nor, however, is there any record evidence that the officers knew this information at the time they seized or searched the computer. Indeed, the evidence indicates that no officer, including the officer who conducted the search of the mirrored hard drive, ever found any indication of password protection. The Government's evidence was that its forensic analysis software would not necessarily detect user passwords.[1]

The district court denied Buckner's motion to suppress and Buckner entered a conditional plea of guilty under Federal Rule of Criminal Procedure 11(a)(2) (2003), reserving the right to appeal the denial of the suppression motion. In the district court, Buckner challenged both the officers' seizure of the computer and the subsequent search of password-protected files located on the computer's hard drive. On appeal, he challenges only the search.

II.

In considering a ruling on a motion to suppress, we review conclusions of law *de novo* and underlying factual findings for clear error. *United States v. Jarrett*, 338 F.3d 339, 343-44 (4th Cir. 2003).

[1]The parties agree that none of Frank Buckner's files were encrypted. Nor is there any contention that the police officers *deliberately* used software that would avoid discovery of any existing passwords.

Although the Fourth Amendment generally prohibits warrantless searches, *see Maryland v. Dyson*, 527 U.S. 465, 466 (1999), valid consent to seize and search items provides an exception to the usual warrant requirement, *see Schneckloth v. Bustamonte*, 412 U.S. 218 (1973). In responding to a defendant's motion to suppress, the Government bears the burden of establishing, by a preponderance of the evidence, that it obtained valid consent to search. *See United States v. Block*, 590 F.2d 535, 539 (4th Cir. 1978).

Consent to search is valid if it is (1) "knowing and voluntary," *Trulock v. Freeh*, 275 F.3d 391, 401 (4th Cir. 2001) (*citing United States v. Mendenhall*, 446 U.S. 544, 557 (1980)), and (2) given by one with authority to consent, *Trulock*, 275 F.3d at 402-03 (*citing Stoner v. California*, 376 U.S. 483 (1964)). There is no question in this case that Michelle Buckner's consent was knowing and voluntary; Frank Buckner challenges only her authority to consent. Because the Government has never contended that Michelle had primary ownership of, or sole access to, these files, this case presents an issue of third-party consent.

A third-party has authority to consent to a search of property when she possesses "common authority over or other sufficient relationship to the . . . effects sought to be inspected." *United States v. Matlock*, 415 U.S. 164, 171 (1975). "Common authority" in this context is not merely a question of property interest. Rather, it requires evidence of "mutual use" by one generally having "joint access or control for most purposes." *Id.* at 171, n.7. Such use makes it "reasonable to recognize that any of the co-[users] has the right to permit the inspection in h[er] own right and that the others have assumed the risk that one of their number might permit the common [effects] to be searched." *Id.*

We have previously considered whether a computer user has actual authority to consent to a warrantless search of the password-protected files of a co-user. In *Trulock*, when considering whether FBI agents were entitled to qualified immunity in a suit alleging a Fourth Amendment violation, we held that a co-resident of a home and co-user of a computer, who did not know the necessary password for her co-user's password-protected files, lacked the authority to consent to a warrantless search of those files. 275 F.3d at 403. Borrowing an analogy from *United States v. Block*, 590 F.2d 535, 539 (4th Cir.

1978), we likened these private files to a "locked box" within an area of common authority. *Trulock*, 275 F.3d at 403-04. Although common authority over a general area confers actual authority to consent to a search of that general area, it does not "automatically . . . extend to the interiors of every discrete enclosed space capable of search within the area." *Block*, 590 U.S. at 541.

The logic of *Trulock* applies equally here. "By using a password," Frank Buckner, like Trulock, "affirmatively intended to exclude . . . others from his personal files." *Trulock*, 275 F.3d at 403. For this reason, "it cannot be said that" Buckner, any more than Trulock, "assumed the risk" that a joint user of the computer, not privy to password-protected files, "would permit others to search his files." *See id.* Thus, under the *Trulock* rationale, Michelle Buckner did not have actual authority to consent to a search of her husband's password-protected files because she did not share "mutual use, general access or common authority" over those files,[2] *United States v. Kinney*, 953 F.2d 863, 866 (4th Cir. 1992).

Michelle's lack of actual authority, however, does not end our inquiry. The Government need not establish that Michelle Buckner had actual authority to consent to a search of Buckner's password-protected files in order to succeed on appeal. Rather, it would be sufficient that Michelle had apparent authority to consent to the search at issue. *See Illinois v. Rodriguez*, 497 U.S. 177, 188 (1990). As long as "the facts available to the officer at the moment . . . 'warrant a [person] of reasonable caution in the belief' that the consenting party had authority," apparent authority to consent exists, and evidence seized or searched pursuant to that consent need not be suppressed. *Id.* (*quoting Terry v. Ohio*, 392 U.S. 1, 21-22 (1968)); *see also Kinney*, 953 F.2d at 866.

[2]The Government argues that because the computer was leased only in Michelle's name, Buckner had no reasonable expectation of privacy in his password-protected files. To be sure, this fact does bear on the reasonableness of an expectation of privacy; but in this case, the district court expressly found that Buckner *did* have a reasonable expectation of privacy in his password-protected files, *see United States v. Buckner*, 407 F.Supp.2d 777, 779 (W.D.Va. 2006), a finding that we cannot hold clearly erroneous.

Michelle gave the officers consent to "take whatever [they] needed [and] whatever [they] found that [they] thought was important to the investigation." This unquestionably provided the officers with valid consent to seize and search any items in the home over which Michelle had common authority. Nevertheless, Frank Buckner contends that Michelle did not have common authority over his computer files — a fact that the officers must have known, according to Buckner, because Michelle had told them that she was not computer-savvy and that she only used the computer to play games.

Whether the officers reasonably believed that Michelle had authority to consent to a search of all the contents of the computer's hard drive, however, depends on viewing these facts in light of the *totality* of the circumstances known to the officers at the time of the search. At that time, the officers knew that the computer was located in a common living area of the Buckners' marital home, they observed that the computer was on and the screen lit despite the fact that Frank Buckner was not present, and they had been told that fraudulent activity had been conducted from that computer using accounts opened in *Michelle*'s name. The officers also knew that the machine was leased solely in *Michelle*'s name and that she had the ability to return the computer to the rental agency at any time, without Frank Buckner's knowledge or consent.

Furthermore, the officers did not have any indication from Michelle, or any of the attendant circumstances, that any files were password-protected. *Cf. Trulock*, 275 F.3d at 398 (noting that the searching officers were explicitly told that the computer contained password-protected files to which the consenting party did not have access). Even during the mirroring and forensic analysis processes, nothing the officers saw indicated that any computer files were encrypted or password-protected.[3] Despite Michelle's suggestion that she lacked deep familiarity with the computer, the totality of the circumstances provided the officers with the basis for an objectively reasonable belief that Michelle had authority to consent to a search of the

[3]We do not hold that the officers could rely upon apparent authority to search while simultaneously using mirroring or other technology to intentionally avoid discovery of password or encryption protection put in place by the user. *See supra* note 1.

computer's hard drive. Therefore, the police were justified in relying on Michelle's consent to search the computer and all of its files, such that no search warrant was required.

III.

For the foregoing reasons, we hold that the officers acted pursuant to a reasonable belief that Michelle Buckner had authority to consent to the contested search. Therefore, the district court's judgment denying Frank Buckner's motion to suppress is

AFFIRMED.