UNITED STATES, Appellee

v.

Jason A. RADER, Airman
U.S. Air Force, Appellant

No. 06-0860

Crim. App. No. 36133

United States Court of Appeals for the Armed Forces

Argued March 12, 2007

Decided May 4, 2007

RYAN, J., delivered the opinion of the Court, in which EFFRON, C.J., and BAKER, ERDMANN, and STUCKY, JJ., joined.

Counsel

For Appellant: Lieutenant Colonel Frank R. Levi (argued); Lieutenant Colonel Mark R. Strickland and Captain Anthony D. Ortiz (on brief).

For Appellee: Colonel Gerald R. Bruce (argued); Major Matthew S. Ward and Captain Jamie L. Mendelson (on brief).

Military Judge: W. Thomas Cumbie

Judge RYAN delivered the opinion of the Court.

A law enforcement officer does not violate the Fourth Amendment's proscription against "unreasonable searches and seizures" where a third party who possesses common authority over the premises or effects consents to the search. United States v. Matlock, 415 U.S. 164, 170-71, (1974); Frazier v. Cupp, 394 U.S. 737, 740 (1969); United States v. Clow, 26 M.J. 176, 183 (1988); Military Rule of Evidence (M.R.E.) 314(e)(2). The question before us is whether Appellant's roommate had sufficient access and control of Appellant's computer to consent to the search and seizure of certain unencrypted files in Appellant's non-password-protected computer. The record supports the military judge's conclusion that the roommate had common authority over Appellant's computer for most purposes, and we affirm the decision of the court below.

A general court-martial composed of a military judge sitting alone convicted Appellant, pursuant to his pleas, of three specifications related to the use of his computer and an interactive computer service to receive child pornography, in violation of Article 134, Uniform Code of Military Justice (UCMJ), 10 U.S.C. § 934 (2000). Prior to his pleas, Appellant moved to suppress the images of child pornography retrieved from his personal computer on the ground that his roommate did not have authority to consent to the search and seizure of his

computer. That motion was denied. Appellant pled guilty, but reserved his right to litigate the military judge's adverse ruling on his motion to suppress by entering a conditional plea pursuant to Rule for Courts-Martial (R.C.M.) 910(a)(2).

The sentence adjudged by the court-martial and approved by the convening authority included a bad-conduct discharge, confinement for nine months, forfeiture of all pay and allowances, and reduction to the lowest enlisted grade. The United States Air Force Court of Criminal Appeals affirmed. United States v. Rader, No. ACM 36133, 2006 CCA LEXIS 164, 2006 WL 1976603 (A.F. Ct. Crim. App. June 20, 2006).

We granted review of the following issue:

> WHETHER THE MILITARY JUDGE ERRED IN ADMITTING EVIDENCE AT TRIAL THAT WAS OBTAINED AS A DIRECT RESULT OF AN ILLEGAL SEARCH OF APPELLANT'S PERSONAL COMPUTER.

United States v. Rader, 64 M.J. 368 (C.A.A.F. 2006).

I. FACTS

A.

Between May and October of 2003, Appellant and two other servicemembers, Airman Thacker and Airman First Class (A1C) Davis, rented an apartment in an off-base apartment complex in Layton, Utah. In May or June, the Appellant agreed to purchase A1C Davis' computer. The computer was originally kept in Appellant's bedroom, but was relocated to A1C Davis' bedroom

after August 2003 due to ventilation problems in Appellant's room.

Both A1C Davis and Airman Thacker used Appellant's computer to play computer games. This access and use was with the knowledge and consent of Appellant. A1C Davis also accessed Appellant's computer approximately every two weeks to perform routine maintenance. Computers owned by A1C Davis, Airman Thacker, and Appellant were joined together by a local access network (LAN), for the purpose of playing games and sharing files.

When recovering from surgery on September 26, 2003, A1C Davis used Appellant's computer, which was located in Davis' bedroom, to perform maintenance, pursuant to Appellant's request. While performing maintenance, A1C Davis opened a folder entitled "My Music." In this folder, A1C Davis noticed thumbnails[1] that appeared to be images of children engaging in sexual acts. Neither the computer nor Appellant's "My Music" folder was password protected. Further, the Appellant never prohibited A1C Davis from accessing the computer or any files within it. Although A1C Davis had never used the LAN to access the Appellant's "My Music" folder, A1C Davis believed that each of the roommates could access all of the files on the other roommates' computers via the LAN.

[1] Thumbnails are smaller screen size version of graphic images.

A1C Davis contacted his first sergeant to disclose what he had seen on Appellant's computer. The Air Force Office of Special Investigations (AFOSI) contacted A1C Davis later that afternoon. A1C Davis told the agents that the computer was in his bedroom; that there was a LAN file sharing system; that Appellant was in the process of purchasing the computer from him but had not yet paid for it completely; and that he did not need permission to use Appellant's computer. A1C Davis repeated all this information to Captain Brock, a judge advocate from the Hill Air Force Base legal office.

Captain Brock and the AFOSI agents accompanied A1C Davis to his apartment, where he gave voluntary consent for the agents to enter and search the apartment and to search the computer. AFOSI agents accessed the computer's files and obtained the child pornography images from the hard drive that formed the basis of the charged offenses against Appellant.

B.

At his court-martial, Appellant moved to suppress the images. At the suppression hearing, the Government presented testimony by A1C Davis, Airman Thacker, Captain Brock, and the special agents that interviewed A1C Davis and monitored a phone

call from A1C Davis to Appellant.[2] Appellant testified for the purposes of the motion only. See M.R.E. 311(f).

The military judge issued findings of fact, from which the factual background detailed above is drawn. See United States v. Reister, 44 M.J. 409, 413 (C.A.A.F. 1996) (stating that in reviewing a ruling on a motion to suppress, we consider the evidence in the light most favorable to the prevailing party). As relevant to the granted issue, the military judge's conclusion of law was that the Government had established by clear and convincing evidence that A1C Davis had sufficient access over the computer to give valid consent to its search.

II. DISCUSSION

We review the denial of a motion to suppress for an abuse of discretion. United States v. Khamsouk, 57 M.J. 282, 286 (C.A.A.F. 2002). Findings of fact are affirmed unless they are clearly erroneous; conclusions of law are reviewed de novo. United States v. Flores, __ M.J. __ (8) (C.A.A.F. 2007) (citing Khamsouk, 57 M.J. at 286).

Ordinarily the search of a home, to include a search of items within the home, such as a computer, is prohibited in the

[2] The parties entered into stipulations of expected testimony for one of the special agents and Airman Thacker. Airman Thacker's stipulation included the facts that he used Appellant's computer to play video games, that Appellant never restricted his access to the computer, and that the computer was never password protected or secured.

absence of a warrant. U.S. Const. amend. IV; Georgia v. Randolph, 126 S. Ct. 1515, 1520 (2006); United States v. Conklin, 63 M.J. 333, 337 (C.A.A.F. 2006) (reaffirming expectation of privacy in the contents of a personal computer). "The prohibition does not apply, however, to situations in which voluntary consent has been obtained." Illinois v. Rodriguez, 497 U.S. 177, 181 (1990). Valid consent to search can be provided, under some circumstances, by a third party. Matlock, 415 U.S. at 170-71; Frazier, 394 U.S. at 740; Clow, 26 M.J. at 183; Reister, 44 M.J. at 414; M.R.E. 314(e)(2).

The validity of the third party consent does not hinge "on niceties of property law or on legal technicalities." Clow, 26 M.J. at 183. Rather, a third party has authority to consent to a search when he possesses "common authority over or other sufficient relationship to the premises or effects sought to be inspected." Matlock, 415 U.S. at 171. That consent "is valid as against the absent, nonconsenting person with whom that authority is shared." Id. at 170; see also Randolph, 126 S. Ct. at 1527 (reaffirming the constitutional sufficiency of third party consent absent the objection of a present, nonconsenting person with whom the authority is shared).

Common authority is "mutual use of the property by persons generally having joint access or control for most purposes, so that it is reasonable to recognize that any of the co-

inhabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit" the search. Matlock, 415 U.S. at 171 n.7. M.R.E. 314(e)(2) recognizes this same concept: a third party "may grant consent to search property when the person exercises control over that property."

"When reviewing a decision of a Court of Criminal Appeals on a military judge's ruling, 'we typically have pierced through that intermediate level' and examined the military judge's ruling, then decided whether the Court of Criminal Appeals was right or wrong in its examination of the military judge's ruling." United States v. Shelton, 64 M.J. 32, 37 (C.A.A.F. 2006) (quoting United States v. Siroky, 44 M.J. 394, 399 (C.A.A.F. 1996)). We agree with the United States Air Force Court of Criminal Appeals that the military judge understood and applied the correct law in determining whether A1C Davis' consent was valid, for purposes of M.R.E. 314(e) and the Fourth Amendment. Rader, 2006 CCA LEXIS 164, at *4, 2006 WL 1976603, at *2.

The military judge correctly stated the Government's burden of proof, focused his factual inquiry specifically on whether A1C Davis had joint access or control over Appellant's computer, and understood the relevant test for determining the validity of a third party's consent.

Appellant nonetheless contends that A1C Davis could not consent to the search of Appellant's computer because he had only limited use and access to it. Consequently, his argument goes, the search was illegal, the images derived from it inadmissible, and the findings and sentence should be set aside. See Wong Sun v. United States, 371 U.S. 471, 485-86 (1963); M.R.E. 311(a).

The control a third party exercises over property or effects is a question of fact. See, e.g., Rodriguez, 497 U.S. at 180 (detailing record facts evidencing control over the premises, and lack thereof). We will not disturb the military judge's findings of fact unless they are clearly erroneous or unsupported by the record. Reister, 44 M.J. at 413.

In this case, the findings of fact include the following: (1) Appellant's computer was physically "located in [A1C] Davis' bedroom"; (2) "[N]either the accused's computer nor the My Music folder on the accused's computer was protected by a password"; (3) "[T]he accused never told Davis not to access his computer or any files within the computer"; (4) A1C Davis and Airman Thacker "used the accused's computer to play computer games" with Appellant's "knowledge and consent"; (5) A1C Davis "accessed the accused's computer approximately every two week[s] to perform routine maintenance on that computer"; and (6)

Appellant "never told Davis not to access his computer or any files within the computer."[3]

We agree with the lower court that the military judge's findings of fact "were well-grounded in the facts developed on the record," Rader, 2006 CCA LEXIS 164, at *4, 2006 WL 1976603, at *2, and Appellant has not demonstrated that they are clearly erroneous. See United States v. Springer, 58 M.J. 164, 167 (C.A.A.F. 2003) ("If the military judge makes findings of fact, we review the findings under a clearly erroneous standard of review."); United States v. Owens, 51 M.J. 204, 209 (C.A.A.F. 1999) ("We review a military judge's evidentiary ruling for abuse of discretion.").

Whether these facts rise to the level of "'joint access or control for most purposes,'" is a question of law. Reister, 44 M.J. at 415 (citation omitted). In this case, the military judge concluded that A1C Davis' consent was valid; that it would be "difficult to imagine how there could have been a greater degree of joint access, mutual use, or control." We agree.

We reject Appellant's argument that A1C Davis did not have control over or authority to consent to a search of the "My Music" files within the computer because he only had permission

[3] It is unclear from the record whether Appellant restricted access to his "My Music" folder via the LAN; even if he had, he placed no restriction on his roommates' access to the "My Music" folder while at his computer.

to use the computer to play games or conduct maintenance. First, the military judge's finding that Appellant did nothing to communicate a restriction regarding access to his computer files to anyone is amply supported by the record. Second, to the extent there was an understanding regarding restricted access to Appellant's computer it was tacit and unclear, as evidenced by A1C Davis and Airman Thacker's use of the computer. This is further illustrated by Appellant's response to A1C Davis' phone call to him.

In that call, A1C Davis told Appellant that he had been looking at Appellant's files and seen "porn." The record demonstrates that Appellant expressed neither surprise that his roommate was looking at the files nor dismay that his roommate disregarded the purported restriction on access to them. We agree with the court below that the evidence supports the conclusion that "the restriction testified to by the appellant never existed." Rader, 2006 CCA LEXIS 164, at *4, 2006 WL 1976603, at *2.

This is not to say that consent to use a computer cannot be limited in scope by its owner to certain applications or files. "In the personal computer context, courts examine whether the relevant files were password-protected or whether the defendant otherwise manifested an intention to restrict third-party access." United States v. Aaron, 33 F. App'x 180, 184 (6th Cir.

2002) (per curiam)(unpublished opinion); see also United States v. Buckner, 473 F.3d 551, 554 (4th Cir. 2007) (using a password showed that defendant affirmatively intended to exclude others from his password-protected files); Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir. 2001) (distinguishing joint access to the computer and its hard drive, for which co-user had authority to consent to search, from password-protected files; with respect to those files, co-user had no common authority where there was no access to the passwords); see also Conklin, 63 M.J. at 337 (holding that, where there is no evidence of shared use or common authority, an individual "has a reasonable expectation of privacy in the files kept on a personally owned computer").

But in this case, neither the computer nor any of its files were password protected, encrypted, or subject to any other technological impediment to review by a person at Appellant's computer. And Appellant never told his roommates not to access his computer or any of its files outside of his presence. The record supports the conclusion that A1C Davis had unrestricted access to Appellant's computer, and that Appellant ceded joint access or control over his computer to A1C Davis "'for most purposes.'" Reister, 44 M.J. at 415 (citation omitted). We agree with the military judge and the Court of Criminal Appeals that A1C Davis had sufficient access to and control over the computer to give valid consent to its search, and that Appellant

assumed the risk he might do so. Matlock, 415 U.S. at 171 n.7; Frazier, 394 U.S. at 740.

III. DECISION

The decision of the United States Air Force Court of Criminal Appeals is affirmed.