F I L E D
United States Court of Appeals
Tenth Circuit

August 24, 2007

Elisabeth A. Shumaker
Clerk of Court

PUBLISH

UNITED STATES COURT OF APPEALS

FOR THE TENTH CIRCUIT

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. RAY ANDRUS, Defendant-Appellant.	No. 06-3094

ORDER

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF KANSAS
(D.C. NO. 05-CR-20032-CM)

Before **TACHA**, Chief Judge, **McKAY,** Senior Circuit Judge**, KELLY**, **HENRY**, **BRISCOE**, **LUCERO, MURPHY**, **HARTZ, O'BRIEN, MCCONNELL, TYMKOVICH, GORSUCH**, and **HOLMES**, Circuit Judges.

The appellant's petition for panel rehearing is denied. Judge McKay voted to grant rehearing.

In denying rehearing, however, the panel majority notes that its opinion is limited to the narrow question of the apparent authority of a homeowner to consent to a search of a computer on premises in the specific factual setting presented, including the undisputed

fact that the owner had access to the computer, paid for internet access, and had an e-mail address used to register on a website providing access to the files of interest to law enforcement.

Among the questions not presented in this matter, and for which there is no factual development in the record, are the extent of capability and activation of password protection or user profiles on home computers, the capability of EnCase software to detect the presence of password protection or a user profile, or the degree to which law enforcement confronts password protection or user profiles on home computers.

Finally, appellant's argument premised on *Kyllo v. United States*, 533 U.S. 27 (2001) was made for the first time in his petition for rehearing and was not initially presented to the panel. The argument is therefore forfeited. *United States v. Charley*, 189 F.3d 1251, 1265, n.16 (10th Cir. 1999).

The request for en banc rehearing was transmitted to all of the judges of the court who are in regular active service. A poll was requested and a majority of the active judges voted to deny the request. Judges Kelly, Lucero, McConnell and Holmes voted to grant rehearing.

Entered for the Court,

ELISABETH A. SHUMAKER
Clerk of Court

F I L E D
United States Court of Appeals
Tenth Circuit

April 25, 2007

Elisabeth A. Shumaker
Clerk of Court

PUBLISH

UNITED STATES COURT OF APPEALS

TENTH CIRCUIT

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. RAY ANDRUS, Defendant-Appellant.	No. 06-3094

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF KANSAS
(D.C. NO. 05-CR-20032-CM)

Melissa Harrison, Assistant Federal Public Defender (David J. Phillips, Federal Public Defender, with her on the briefs), Kansas City, Kansas, for Defendant-Appellant.

Leon J. Patton, Assistant United States Attorney (Eric F. Melgren, United States Attorney, with him on the brief), Kansas City, Kansas, for Plaintiff-Appellee.

Before **MURPHY**, **McKAY**, and **GORSUCH**, Circuit Judges.

MURPHY, Circuit Judge.

I. Introduction

Defendant-Appellant Ray Andrus was indicted on one count of possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B). Agents of the Bureau of Immigration and Customs Enforcement ("ICE") found pornographic images of children on Andrus' home computer after Andrus' father, Dr. Bailey Andrus, consented to a search of the Andrus home and Andrus' computer. Andrus moved to suppress the inculpatory evidence found on his computer during the search, arguing Dr. Andrus' consent was not voluntary and that Dr. Andrus lacked both actual and apparent authority to consent to a search of the computer. The district court determined Dr. Andrus' consent was voluntary and that Dr. Andrus had apparent authority to consent to the search. The district court, accordingly, denied Andrus' motion to suppress.

After the district court's denial of his motion, Andrus pleaded guilty to the charge against him but retained the right to appeal the district court's denial of his suppression motion. He was sentenced to seventy months' imprisonment followed by three years' supervised release. In this appeal, Andrus challenges the district court's denial of his suppression motion. Exercising jurisdiction under 28 U.S.C. § 1291, this court concludes Dr. Andrus had apparent authority to consent to a search of Ray Andrus' computer. We therefore **affirm** the district court's denial of Andrus' motion to suppress.

II. Background

Federal authorities first became interested in Ray Andrus during an investigation of Regpay, a third-party billing and credit card aggregating company that provided subscribers with access to websites containing child pornography. The investigation of Regpay led to an investigation of Regpay subscribers. One of the subscribers providing personal information and a credit card number to Regpay was an individual identifying himself as "Ray Andrus" at "3208 W. 81st Terr., Leawood, KS." The Andrus Regpay subscription was used to access a pornographic website called www.sunshineboys.com. Record checks with the drivers license bureau and post office indicated Ray Andrus, Bailey Andrus, and a third man, Richard Andrus, all used the West 81st Terrace address. The credit card number provided to Regpay was determined to belong to Ray Andrus. The email address provided to Regpay, "bandrus@kc.rr.com," was determined to be associated with Dr. Bailey Andrus.

The federal investigation into the Andrus household began in January 2004 and focused primarily on Ray Andrus. At least one agent conducted surveillance on the Andrus residence and knew Ray Andrus worked at the Shawnee Mission School. Eight months into the investigation, agents believed they did not have enough information to obtain a search warrant for the Andrus residence. They, therefore, attempted to gather more information by doing a "knock and talk" interview with the hope of being able to conduct a consent search. ICE Special Agent Cheatham and Leawood Police Detective Woollen arrived at the Andrus house at approximately 8:45 a.m. on August 27, 2004.

ICE Special Agent Kanatzar, a forensic computer expert, accompanied Cheatham and Woollen to the residence, but waited outside in his car for Cheatham's authorization to enter the premises.

Dr. Andrus, age ninety-one, answered the door in his pajamas. Dr. Andrus invited the officers into the residence and, according to the testimony of Cheatham and Woollen, the three sat in Dr. Andrus' living room, where the officers learned that Ray Andrus lived in the center bedroom in the residence. In response to the officers' questions, Dr. Andrus indicated Ray Andrus did not pay rent and lived in the home to help care for his aging parents. Cheatham testified he could see the door to Ray Andrus' bedroom was open and asked Dr. Andrus whether he had access to the bedroom. Dr. Andrus testified he answered "yes" and told the officers he felt free to enter the room when the door was open, but always knocked if the door was closed.

Cheatham asked Dr. Andrus for consent to search the house and any computers in it. Dr. Andrus signed a written consent form indicating his willingness to consent to a premises and computer search. He led Cheatham into Ray Andrus' bedroom to show him where the computer was located. After Dr. Andrus signed the consent form, Cheatham went outside to summon Kanatzar into the residence. Kanatzar went straight into Andrus' bedroom and began assembling his forensic equipment. Kanatzar removed the cover from Andrus' computer and hooked his laptop and other equipment to it. Dr. Andrus testified he was present at the beginning of the search but left the bedroom shortly thereafter. Kanatzar testified it took about ten to fifteen minutes to connect his equipment

before he started analyzing the computer. Kanatzar used EnCase forensic software to examine the contents of the computer's hard drive. The software allowed him direct access to the hard drive without first determining whether a user name or password were needed. He, therefore, did not determine whether the computer was protected by a user name or password prior to previewing the computer's contents. Only later, when he took the computer back to his office for further analysis, did he see Ray Andrus' user profile.[1]

Kanatzar testified he used EnCase to search for .jpg picture files.[2] He explained that clicking on the images he retrieved allowed him to see the pathname for the image, tracing it to particular folders on the computer's hard drive. This process revealed folder and file names suggestive of child pornography. Kanatzar estimated it took five minutes to see depictions of child pornography. At that point, however, Cheatham came back into the room, told Kanatzar that Ray Andrus was on his way home, and asked Kanatzar to stop the search. Kanatzar testified he shut down his laptop computer and waited in Ray Andrus' bedroom with the computer until Cheatham came back into the room to tell him Andrus had personally consented to the search and Kanatzar could continue.

Cheatham testified he asked Kanatzar to stop the computer search because of information revealed through his continuing conversation with Dr. Andrus. Cheatham

---

[1]Kanatzar testified that someone without forensic equipment would need Ray Andrus' user name and password to access files stored within Andrus' user profile.

[2]JPEG is a commonly used method for compressing and storing electronic photographic images. JPEG files are usually saved with the ".jpg" extension appended to the computer file name and indicate the file contains a photograph or graphical image. *See United States v. Walser*, 275 F.3d 981, 984 n.3 (10th Cir. 2001).

explained he asked Dr. Andrus if there were other computers in the house and Dr. Andrus replied the computer in Ray Andrus' room was the only one. Cheatham then asked Dr. Andrus about the internet service and Dr. Andrus indicated it was part of the cable package. At that point, Ray Andrus was telephoned at his workplace. There is conflicting evidence concerning whether Dr. Andrus or Cheatham suggested calling Andrus. Dr. Andrus dialed Andrus' work number, spoke briefly with his son, and handed the phone to Cheatham.[3] At the conclusion of his conversation with Cheatham, Ray Andrus agreed to return to the Andrus residence. He arrived ten to twenty minutes later. He parked his car in the garage and was met by Cheatham, Woollen, and ICE Agent Smith, who arrived on the scene after the agents' initial entry into the Andrus residence. Cheatham testified he told Andrus that officers had already been inside the residence and had looked through his room. Cheatham's written report also indicates he told Andrus he had a computer technician at the residence and that Dr. Andrus had consented to a search of the house and the computer in Andrus' bedroom. Cheatham said he then verbally asked Andrus for consent to search his room and his computer. After obtaining Andrus' consent, Cheatham went back inside to authorize Kanatzar to continue his search.

---

[3]It is disputed whether Cheatham told Andrus during this phone call that child pornography had been found on his computer. Cheatham maintained he did not mention to Andrus that the computer search was already underway, while Andrus testified Cheatham told him during the phone call that pornography had been discovered during a search of his computer. Because of the conclusion that Dr. Andrus had apparent authority to consent to a search of the computer, we need not analyze the voluntariness of Ray Andrus' subsequent consent and, therefore, need not address the district court's resolution of this factual dispute.

Ray Andrus was indicted on one count of knowingly and intentionally possessing pornographic images of minors in violation of 18 U.S.C. § 2252(a)(4)(B).[4] Claiming a Fourth Amendment violation, Andrus moved to suppress the evidence gathered from his residence and his computer. In the memorandum supporting his motion to suppress, Andrus argued: (1) Dr. Andrus' consent was not voluntary; (2) Dr. Andrus lacked actual authority to consent to a search of the computer, even if he had authority to consent to a search of Ray Andrus' room; and (3) Dr. Andrus could not reasonably be seen as having authority to consent to a search of the computer and, thus, lacked apparent authority.

The district court held an evidentiary hearing at which Detective Woollen, Agent Cheatham, Agent Kanatzar, Agent Smith, Dr. Andrus, and Ray Andrus testified. At the conclusion of the hearing, the court determined Dr. Andrus' consent was voluntary, but concluded Dr. Andrus lacked actual authority to consent to a computer search. The court based its actual authority ruling on its findings that Dr. Andrus did not know how to use the computer, had never used the computer, and did not know the user name that would have allowed him to access the computer.

The district court then proceeded to consider apparent authority. It indicated the resolution of the apparent authority claim in favor of the government was a "close call."

---

[4]18 U.S.C. § 2552(a)(4)(B) criminalizes "possess[ion of] 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported in interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if—(i) the producing of such visual depiction involves the use of a minor engaging in explicit conduct; and (ii) such visual depiction is of such conduct."

The court concluded the agents' belief that Dr. Andrus had authority to consent to a search of the computer was reasonable up until the time they learned there was only one computer in the house. Because Cheatham instructed Kanatzar to suspend the search at that point, there was no Fourth Amendment violation. The court based its conclusion that Dr. Andrus had apparent authority on the following factual findings: (1) the email address bandrus@kc.rr.com, an address associated with Dr. Bailey Andrus, was used to register with Regpay and procure child pornography; (2) Dr. Andrus told the agents he paid the household's internet access bill; (3) the agents knew several individuals lived in the household; (4) Ray Andrus' bedroom door was not locked, leading a reasonable officer to believe other members of the household could have had access to it; and (5) the computer itself was in plain view of anyone who entered the room and it appeared available for anyone's use. Implicit in the district court's analysis was the assumption that the officers could reasonably have believed Dr. Andrus accessed the internet through the computer in Ray Andrus' bedroom, thereby giving Dr. Andrus the authority to consent to a search of the computer.

Lastly, the court concluded Ray Andrus' later consent to search his computer and his admissions regarding additional evidence were knowing and voluntary. It found the agents had explained they were investigating violations of federal law regarding child pornography, advised Andrus of the circumstances facing him, and told him he was not under arrest and was free to go at any time. The court further found that Andrus told the agents he wanted to clear up the matter and gave consent to search his computer. Based

on these factual findings, the court concluded Andrus' consent was given knowingly and voluntarily. The district court denied Andrus' motion to suppress.

On appeal, Andrus contests the district court's apparent authority ruling. He contends that ambiguities in the situation facing the officers at the Andrus residence required the officers to ask further questions concerning Dr. Andrus' authority to consent to a computer search prior to commencing the search. *See United States v. Kimoana*, 383 F.3d 1215, 1222 (10th Cir. 2004). Andrus also argues on appeal that his own consent, given after the allegedly illegal computer search yielded inculpatory evidence, did not cure the alleged illegality because the earlier search and his later consent were not sufficiently attenuated. *See United States v. Melendez-Garcia*, 28 F.3d 1046,1053–54 (10th Cir. 1994).

For the reasons explained below, this court concludes Dr. Andrus had apparent authority to consent to the computer search. Because there was, therefore, no constitutional taint associated with the initial search and because Ray Andrus does not draw a distinction between evidence seized during the initial search and evidence seized after he arrived home, the validity of Andrus' subsequent consent need not be addressed.

III. Discussion

A. Standard of Review

When reviewing a district court's denial of a motion to suppress, this court considers the totality of the circumstances and views the evidence in the light most favorable to the

government. *Kimoana*, 383 F.3d at 1220. We accept the district court's factual findings unless they are clearly erroneous. *Id.* Consideration of witness credibility, the weight given to evidence, and reasonable inferences drawn from evidence are within the district court's province as the fact-finder. *Id*. Issues of law, however, such as determinations of reasonableness under the Fourth Amendment and the validity of consent, are reviewed *de novo*. *United States v. Mitchell*, 429 F.3d 952, 960 (10th Cir. 2005); *United States v. Rith*, 164 F.3d 1323, 1328 (10th Cir. 1999).

B. Consent Searches Under the Fourth Amendment

Subject to limited exceptions, the Fourth Amendment prohibits warrantless searches of an individual's home or possessions. *Illinois v. Rodriguez*, 497 U.S. 177, 181 (1990). Voluntary consent to a police search, given by the individual under investigation or by a third party with authority over the subject property, is a well-established exception to the warrant requirement. *Rith*, 164 F.3d at 1328. Valid third party consent can arise either through the third party's actual authority or the third party's apparent authority. A third party has actual authority to consent to a search "if that third party has either (1) mutual use of the property by virtue of joint access, or (2) control for most purposes." *Id.* at 1329*; see also United States v. Matlock*, 415 U.S. 164, 171 (1974) (holding "common authority over or other sufficient relationship to the premises or effects sought to be inspected" may give rise to a third party's valid consent to search). Even where actual authority is lacking, however, a third party has apparent authority to consent to a search when an officer reasonably, even if erroneously, believes the third party possesses

authority to consent. *See Georgia v. Randolph*, 126 S. Ct. 1515, 1520 (2006).

Whether apparent authority exists is an objective, totality-of-the-circumstances inquiry into whether the facts available to the officers at the time they commenced the search would lead a reasonable officer to believe the third party had authority to consent to the search. *See Rodriguez*, 497 U.S. at 188; *Kimoana*, 383 F.3d at 1222 ("[W]here an officer is presented with ambiguous facts related to authority, he or she has a duty to investigate further before relying on the consent."). When the property to be searched is an object or container, the relevant inquiry must address the third party's relationship to the object. *Matlock*, 415 U.S. at 171. The Supreme Court's most recent pronouncement on third party consent searches underscores that reasonableness calculations must be made in the context of social expectations about the particular item to be searched. *Randolph*, 126 S. Ct. at 1521. In *Randolph*, the Court explained, "The constant element in assessing Fourth Amendment reasonableness in consent cases . . . is the great significance given to widely shared social expectations." *Id.* For example, the Court said, "[W]hen it comes to searching through bureau drawers, there will be instances in which even a person clearly belonging on the premises as an occupant may lack any perceived authority to consent." *Id.* at 1522.

Objects typically associated with high expectations of privacy include "mankind's valises, suitcases, footlockers, [and] strong boxes." *United States v. Block*, 590 F.2d 535, 541 (4th Cir. 1978); *see United States v. Salinas-Cano*, 959 F.2d 861, 865 (10th Cir. 1992) (contrasting a suitcase, in which defendant had a high expectation of privacy, with

a cardboard box, cassette tape, or plastic bucket, with which lesser expectations of privacy are associated). It may be unreasonable for law enforcement to believe a third party has authority to consent to the search of an object typically associated with a high expectation of privacy, especially when the officers know or should know the owner has indicated the intent to exclude the third party from using or exerting control over the object. *See Salinas-Cano*, 959 F.2d at 865–66 (determining officers' belief in apartment owners' authority to consent to search of defendant's suitcase to be unreasonable where police failed to inquire into apartment owner's use of or control over the suitcase).

This court has not previously considered expectations of privacy associated with a home computer in a third party consent situation. Tenth Circuit precedent thus far has dealt only with computer searches where police have a warrant or other justification for searching the computer, or when the defendant computer owner himself has consented to the search. *See, e.g.*, *United States v. Brooks*, 427 F.3d 1246,1249–53 (10th Cir. 2005) (concluding defendant's consent to search of his computer authorized law enforcement's search); *United States v. Tucker*, 305 F.3d 1193, 1202 (10th Cir. 2002) (concluding parole search of defendant's computer was permitted by the plain language of defendant's parole agreement); *United States v. Carey*, 172 F.3d 1268, 1276 (10th Cir. 1999) (determining officer exceeded scope of warrant authorizing computer search for evidence of drug crimes when officer found and continued to search for child pornography on defendant's computer). Other courts have, however, analyzed third party authority to consent to the search of a home computer, focusing on the application of Fourth Amendment principles

in this special case where it is unclear from a visual inspection of the outside of the computer whether the computer's owner has manifested a subjective expectation of privacy in the computer or its data.

1. Analogizing Computers to Other Types of Containers

Courts considering the issue have attempted to analogize computers to other items more commonly seen in Fourth Amendment jurisprudence. Individuals' expectations of privacy in computers have been likened to their expectations of privacy in "a suitcase or briefcase." *United States v. Aaron*, 33 F. App'x 180, 184 (6th Cir. 2006) (unpublished). Password-protected files have been compared to a "locked footlocker inside the bedroom." *Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001).

Given the pervasiveness of computers in American homes, this court must reach some, at least tentative, conclusion about the category into which personal computers fall. A personal computer is often a repository for private information the computer's owner does not intend to share with others.

> [F]or most people, their computers are their most private spaces. People commonly talk about the bedroom as a very private space, yet when they have parties, all the guests—including perfect strangers —are invited to toss their coats on the bed. But if one of those guests is caught exploring the host's computer, that will be his last invitation.

United States v. Gourde, 440 F.3d 1065, 1077 (9th Cir. 2006) (en banc) (Kleinfeld, J., dissenting). *See generally* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 569 (2005) ("[C]omputers are playing an ever greater role in daily life and are recording a growing proportion of it . . . . [T]hey are postal services, playgrounds,

jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more. . . . Each new software application means another aspect of our lives monitored and recorded by our computers."). Because 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." *Salinas-Cano*, 959 F.2d at 864.

2. Manifestations of Expectations of Privacy in Computer Data

The inquiry into whether the owner of a highly personal object has indicated a subjective expectation of privacy traditionally focuses on whether the subject suitcase, footlocker, or other container is physically locked. *See, e.g.*, *Block*, 590 F.2d at 537 (holding mother lacked authority to consent to search of son's footlocker where "[t]he trunk was fastened shut by some means that indicated to the officers that it was locked and that a key was required to open it."). Determining whether a computer is "locked," or whether a reasonable officer should know a computer may be locked, presents a challenge distinct from that associated with other types of closed containers. Unlike footlockers or suitcases, where the presence of a locking device is generally apparent by looking at the item, a "lock" on the data within a computer is not apparent from a visual inspection of the outside of the computer, especially when the computer is in the "off" position prior to the search. Data on an entire computer may be protected by a password, with the password functioning as a lock, or there may be multiple users of a computer, each of whom has an individual and personalized password-protected "user profile." *See* Oxford

English Dictionary Online, http://dictionary.oed.com (last visited Dec. 22, 2006) (entry for "Password," definition 1.b.: defining "password" in the computing context as "[a] sequence of characters, known only to authorized persons, which must be keyed in to gain access to a particular computer, network, file, function, etc."). The presence of a password that limits access to the computer's contents may only be discovered by starting up the machine or attempting to access particular files on the computer as a normal user would.[5]

Courts addressing the issue of third party consent in the context of computers, therefore, have examined officers' knowledge about password protection as an indication of whether a computer is "locked" in the way a footlocker would be. For example, in *Trulock*, the Fourth Circuit held a live-in girlfriend lacked actual authority to consent to a search of her boyfriend's computer files where the girlfriend told police she and her boyfriend shared the household computer but had separate password-protected files that were inaccessible to the other. 275 F.3d at 398, 403. The court in that case explained, "Although Conrad had authority to consent to a general search of the computer, her authority did not extend to Trulock's password-protected files." *Id.* at 403. In *United States v. Morgan*, the Sixth Circuit viewed a wife's statement to police that she and her

[5]The difficulty with seeing a "lock" on computer data is exacerbated by the forensic software sometimes used by law enforcement to conduct computer searches. The software, like the EnCase software used by Agent Kanatzar, allows user profiles and password protection to be bypassed. *See, e.g.*, *United States v. Buckner*, 473 F.3d 551, 553 (4th Cir. 2007) (stating government's evidence was that forensic software "would not necessarily detect user passwords" on password-protected computer files).

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 (6th Cir. 2006). *Accord Aaron*, 33 F. App'x at 184 (determining live-in girlfriend could give valid consent for search of defendant's computer because defendant had not forbidden her from using computer or "restricted her access with password protections"). A critical issue in assessing a third party's apparent authority to consent to the search of a home computer, therefore, is whether law enforcement knows or should reasonably suspect because of surrounding circumstances that the computer is password protected.

3. Additional Factors Bearing on Third Party Consent for Computer Search

In addition to password protection, courts also consider the location of the computer within the house and other indicia of household members' access to the computer in assessing third party authority. Third party apparent authority to consent to a search has generally been upheld when the computer is located in a common area of the home that is accessible to other family members under circumstances indicating the other family members were not excluded from using the computer. *See United States v. Buckner*, 473 F.3d 551, 555–56 (4th Cir. 2007) (determining wife's consent was valid where wife leased computer in her name, wife occasionally used computer, computer was found in living room, and fraudulent activity had been conducted from that computer using accounts opened in wife's name); *Morgan*, 435 F.3d at 663–64 (concluding wife had apparent authority because she initiated contact with police, computer was located in

common area of the house, and wife told police she had used computer, she and husband did not have usernames or passwords, and she had installed software on the computer); *United States v. Smith*, 27 F. Supp. 2d 1111, 1116 (C.D. Ill. 1998) (concluding live-in girlfriend had actual and apparent authority to consent to search of defendant's computer because girlfriend gave police permission to enter house and search computer and computer and desk were in common area and surrounded by children's toys). In contrast, where the third party has affirmatively disclaimed access to or control over the computer or a portion of the computer's files, even when the computer is located in a common area of the house, courts have been unwilling to find third party authority. *Trulock*, 275 F.3d at 403.

C. Dr. Andrus' Apparent Authority to Consent to a Search of Ray Andrus' Computer

Andrus' case presents facts that differ somewhat from those in other cases. Andrus' computer was located in a bedroom occupied by the homeowner's fifty-one year old son rather than in a true common area. *Cf. Morgan*, 435 F.3d at 662 (computer in basement); *Smith*, 27 F. Supp. 2d at 1113 (computer in joint bedroom of girlfriend and defendant, surrounded by children's toys). Dr. Andrus, however, had unlimited access to the room. Law enforcement officers did not ask specific questions about Dr. Andrus' use of the computer, but Dr. Andrus said nothing indicating the need for such questions. *Cf. Trulock*, 275 F.3d at 398 (when law enforcement questioned third party girlfriend about computer, she indicated she and boyfriend had separate password-protected files). The resolution of this appeal turns on whether the officers' belief in Dr. Andrus' authority was

reasonable, despite the lack of any affirmative assertion by Dr. Andrus that he used the computer and despite the existence of a user profile indicating Ray Andrus' intent to exclude other household members from using the computer.[6] For the reasons articulated below, this court concludes the officers' belief in Dr. Andrus' authority was reasonable.

The critical issue in our analysis is whether, under the totality of the circumstances known to Cheatham, Woollen, and Kanatzar, these officers could reasonably have believed Dr. Andrus had authority to consent to a search of the computer. *See Kimoana*, 383 F.3d at 1223. Phrased in the negative, we must ask "whether the surrounding circumstances could conceivably be such that a reasonable person would doubt [Dr. Andrus' consent] and not act upon it without further inquiry." *Rodriguez*, 497 U.S. at 188. If the circumstances reasonably indicated Dr. Andrus had mutual use of or control over the computer, the officers were under no obligation to ask clarifying questions, *cf. Kimoana*, 383 F.3d at 1222, even if, as the dissent notes, the burden would have been minimal in this particular case.

This court must accept the factual findings of the district court unless those findings are clearly erroneous. *Id.* at 1220. We, therefore, accept the following facts as true: First, the officers knew Dr. Andrus owned the house and lived there with family

---

[6]Although the district court did not make any factual findings as to whether the computer was password protected, there is evidence in the record suggesting the presence of a password. *See supra* note 1. Determining whether a password was actually in place, however, is unnecessary for analyzing Dr. Andrus' apparent authority, since the password would not have been obvious to the officers at the time they obtained consent and commenced the search.

members. Second, the officers knew Dr. Andrus' house had internet access and that Dr. Andrus paid the Time Warner internet and cable bill. Third, the officers knew the email address bandrus@kc.rr.com had been activated and used to register on a website that provided access to child pornography. Fourth, although the officers knew Ray Andrus lived in the center bedroom, they also knew that Dr. Andrus had access to the room at will. Fifth, the officers saw the computer in plain view on the desk in Andrus' room and it appeared available for use by other household members. Furthermore, the record indicates Dr. Andrus did not say or do anything to indicate his lack of ownership or control over the computer when Cheatham asked for his consent to conduct a computer search.[7] It is uncontested that Dr. Andrus led the officers to the bedroom in which the computer was located, and, even after he saw Kanatzar begin to work on the computer, Dr. Andrus remained silent about any lack of authority he had over the computer. Even if Ray Andrus' computer was protected with a user name and password, there is no indication in the record that the officers knew or had reason to believe such protections were in place.

Andrus argues his computer's password protection indicated his computer was "locked" to third parties, a fact the officers would have known had they asked questions

---

[7]The district court recognized a conflict in the testimony of Dr. Andrus and Cheatham as to whether Dr. Andrus told Cheatham he did not know how to use the computer prior to Cheatham asking for Dr. Andrus' consent. Taking the evidence in the light most favorable to the government and deferring to the district court's evaluation of witness credibility as we must, *United States v. Kimoana*, 383 F.3d 1215, 1220 (10th Cir. 2004), we too credit the officers' version.

of Dr. Andrus prior to searching the computer. Under our case law, however, officers are not obligated to ask questions unless the circumstances are ambiguous. *Kimoana*, 383 F.3d at 1222. In essence, by suggesting the onus was on the officers to ask about password protection prior to searching the computer, despite the absence of any indication that Dr. Andrus' access to the computer was limited by a password, Andrus necessarily submits there is inherent ambiguity whenever police want to a search a household computer and a third party has not affirmatively provided information about his own use of the computer or about password protection. Andrus' argument presupposes, however, that password protection of home computers is so common that a reasonable officer ought to know password protection is likely. Andrus has neither made this argument directly nor proffered any evidence to demonstrate a high incidence of password protection among home computer users. The dissent, however, is critical of this court because it neither makes the argument for Andrus nor supplies the evidence to support the argument. The key aspect of the dissent is its criticism of the majority for refusing to "take judicial notice that password protection is a standard feature of operating systems." *Post* at 2. A judicially noticed fact is "one not subject to reasonable dispute in that it is either (1) generally known . . . or (2) capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned." Fed. R. Evid. 201(b). Although judicial notice may be taken *sua sponte*, Fed. R. Evid. 201(c), it would be particularly inappropriate for the court to wander undirected in search of evidence irrefutably establishing the facts necessary to support the dissent's conclusion regarding

the absence of apparent authority: namely, that (a) password protection is a standard feature of most operating systems, (b) most users activate the standard password-protection feature, and (c) these are matters of such common knowledge that a reasonable officer would make further inquiry. In rejecting this challenge, the court notes the dissent itself did not take up the search for facts that would meet the requirements of Rule 201(b). Without a factual basis on which to proceed, we are unable to address the possibility that passwords create inherent ambiguities.[8]

Viewed under the requisite totality-of-the-circumstances analysis, the facts known to the officers at the time the computer search commenced created an objectively reasonable perception that Dr. Andrus was, at least, *one* user of the computer. That objectively reasonable belief would have been enough to give Dr. Andrus apparent authority to consent to a search. *See id.* at 1222; *cf. United States v. Durham*, No. 98-10051-02, 1998 WL 684241, at *3–4 (D. Kan. Sept. 11, 1998) (unpublished) (holding mother lacked actual and apparent authority to consent to search of computer in son's room where officers knew room was locked and mother could not produce the correct key). Even if Dr. Andrus had no actual ability to use the computer and the computer was password protected, these mistakes of fact do not negate a determination of Dr. Andrus' apparent authority. *See Rodriguez*, 497 U.S. at 185; *Salinas-Cano*, 959 F.2d at 865–66. Any after-acquired factual knowledge that "might undermine the initial reasonable conclusion of

[8]If the factual basis were provided, law enforcement's use of forensic software like EnCase, which overrides any password protection without ever indicating whether such protection exists, may well be subject to question. This, however, is not that case.

third-party apparent authority [is] generally immaterial." *Morgan*, 435 F.3d at 664. In this case, the district court found Agent Cheatham properly halted the search when further conversation with Dr. Andrus revealed he did not use the computer and that Andrus' computer was the only computer in the house. These later revelations, however, have no bearing on the reasonableness of the officers' belief in Dr. Andrus' authority at the outset of the computer search.

IV. Conclusion

For the foregoing reasons, this court concludes Dr. Andrus had apparent authority to consent to a search of the computer in Ray Andrus' bedroom. Andrus' arguments related to the validity of his subsequent consent, therefore, need not be addressed. We accordingly **affirm** the district court's denial of Andrus' motion to suppress.

06-3094, *United States v. Andrus*

McKAY, Circuit Judge, *dissenting*.

This case concerns the reasonable expectation of privacy associated with password-protected computers. In examining the contours of a third party's apparent authority to consent to the search of a home computer, the majority correctly indicates that the extent to which law enforcement knows or should reasonably suspect that password protection is enabled is critical. We differ, however, over the extent to which the burden of inquiry should rest with law enforcement personnel. More specifically, I take issue with the majority's implicit holding that law enforcement may use software deliberately designed to automatically bypass computer password protection based on third-party consent without the need to make a reasonable inquiry regarding the presence of password protection and the third party's access to that password.

Given the majority's correct decision to categorize computers as containers, with all the attendant protections afforded under the case law, whether a computer search is objectively reasonable depends upon fact-specific determinations in individual cases with no bright-line rules. The few cases confronting this issue pay particular attention to the presence or absence of password protection.[1] *See ante* at 18 (collecting cases).

[1] This scenario appears to present itself infrequently, likely because the majority of computer searches occur pursuant to a search warrant.

The presence of security on Defendant's computer is undisputed.[2] (Suppression Hr'g Tr. at 89.) Yet, the majority curiously argues that Defendant's use of password protection is inconsequential because Defendant failed to argue that computer password protection is "commonplace." *Ante* at 23-24. Of course, the decision provides no guidance on what would constitute sufficient proof of the prevalence of password protection, nor does it explain why the court could not take judicial notice that password protection is a standard feature of operating systems. Despite recognizing the "pervasiveness of computers in American homes," *ante* at 15, and the fact that the "personal computer is often a repository for private information the computer's owner does not intend to share with others," *id.*, the majority requires the invocation of magical language in order to give effect to Defendant's subjective intent to exclude others from accessing the computer.

The development of computer password technology no doubt "presents a challenge distinct from that associated with other types of" *locked* containers. *Ante* at 16-17. But this difficulty does not and cannot negate Fourth Amendment protection to computer storage nor render an expectation of computer privacy unreasonable. *Cf. United States v. Salinas-Cano*, 959 F.2d 861, 864 (10th Cir. 1992) (considering, in assessing appeal of suppression motion, "the precautions taken by the owner to manifest his subjective expectation of privacy, for example locking the container"); *see also Georgia v. Randolph*, 547 U.S. 103, 126 S. Ct. 1515, 1535 (2006) (Roberts, C.J., dissenting) ("To the

[2] The majority suggests otherwise at certain points in its opinion, only to recognize the existence of password protection at other points. *See ante* at 5 n.1, 21-23.

extent a person wants to ensure that his possessions will be subject to a consent search only due to his *own* consent, he is free to place these items in an area over which others do not share access and control, be it a private room or a locked suitcase under a bed."). The unconstrained ability of law enforcement to use forensic software such as the EnCase program to bypass password protection without first determining whether such passwords have been enabled does not "exacerbate[]" this difficulty, *ante* at 17 n.5; rather, it avoids it altogether, simultaneously and dangerously sidestepping the Fourth Amendment in the process. Indeed, the majority concedes that if such protection were "shown to be commonplace, law enforcement's use of forensic software like EnCase . . . may well be subject to question." *Ante* at 24 n.8. But the fact that a computer password "lock" may not be *immediately* visible does not render it unlocked. I appreciate that unlike the locked file cabinet, computers have no handle to pull. But, like the padlocked footlocker, computers do exhibit outward signs of password protection: they display boot password screens, username/password log-in screens, and/or screen-saver reactivation passwords.[3]

The fact remains that EnCase's ability to bypass security measures is well known to law enforcement. Here, ICE's forensic computer specialist found Defendant's computer turned off. Without turning it on, he hooked his laptop directly to the hard drive of Defendant's computer and ran the EnCase program. The agents made no effort to

[3] I recognize that the ability of users to program automatic log-ins and the capability of operating systems to "memorize" passwords poses potential problems, since these only create the appearance of a restriction without actually blocking access.

ascertain whether such security was enabled prior to initiating the search. The testimony makes clear that such protection was discovered during additional computer analysis conducted at the forensic specialist's office. *Cf. United States v. Buckner*, 473 F.3d 551, 555 & n.3 (4th Cir. 2007) (hinting that objectively reasonable belief in valid third-party consent could be tainted by unnoticed presence of password protection and therefore limiting its holding to prevent "[reliance] 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").

The majority points out that law enforcement "did not ask specific questions" about Dr. Andrus' use of the computer or knowledge of Ray Andrus' use of password protection, *ante* at 20, but twice criticizes Dr. Andrus' failure to affirmatively disclaim ownership of, control over, or knowledge regarding the computer. Of course, the computer was located in Ray Andrus' very tiny bedroom, but the majority makes no effort to explain how this does not create an ambiguous situation as to ownership. *Cf. Buckner*, 473 F.3d at 555 (computer located in common living area); *United States v. Morgan*, 435 F.3d 660, 662, 663 (6th Cir. 2006) (same); *United States v. Aaron*, 33 Fed. App'x 180, 182 (6th Cir. 2002) (unpublished) (computer located in unlocked spare bedroom); *Trulock v. Freeh*, 275 F.3d 391, 398 (4th Cir. 2001) (computer located in consenter's bedroom); *United States v. Smith*, 27 F. Supp. 2d 1111, 1116 (C.D. Ill. 1998) (computer located in master bedroom alcove that defendant shared with consenter and consenter's children).

The burden on law enforcement to identify ownership of the computer was minimal. A simple question or two would have sufficed. Prior to the computer search, the agents questioned Dr. Andrus about Ray Andrus' status as a renter and Dr. Andrus' ability to enter his 51-year-old son's bedroom in order to determine Dr. Andrus' ability to consent to a search of the room, but the agents did not inquire whether Dr. Andrus used the computer, and if so, whether he had access to his son's password. At the suppression hearing, the agents testified that they were not immediately aware that Defendant's computer was the only one in the house, and they began to doubt Dr. Andrus' authority to consent when they learned this fact. The record reveals that, upon questioning, Dr. Andrus indicated that there was a computer in the house and led the agents to Defendant's room. The forensic specialist was then summoned. It took him approximately fifteen to twenty minutes to set up his equipment, yet, bizarrely, at no point during this period did the agents inquire about the presence of any other computers. The consent form, which Dr. Andrus signed prior to even showing the agents Defendant's computer, indicates that Dr. Andrus consented to the search of only a single "computer," rather than computers. In addition, the local police officer accompanying the ICE agents heard Dr. Andrus tell his wife that the agents wanted to search *Defendant's* computer, which would have caused a reasonable law enforcement official to question Dr. Andrus' ownership and use of the computer.

The record reflects that, even prior to the agent's arrival at the target home, the agents

were cognizant of the ambiguity surrounding the search.[4] The agents testified that they suspended their search due to doubts regarding Dr. Andrus' ability to consent only after they learned that the internet service used by Defendant came bundled with the cable television service and was paid by Dr. Andrus. The district court noted, however, that the agents were aware of this fact prior to the search, having subpoenaed the internet/cable records from the service provider prior to their "knock-and-talk." Given the inexcusable confusion in this case, the circumstantial evidence is simply not enough to justify the agents' use of EnCase software without making further inquiry.

Accordingly, in my view, given the case law indicating the importance of computer password protection, the common knowledge about the prevalence of password usage, and the design of EnCase or similar password bypass mechanisms, the Fourth Amendment and the reasonable inquiry rule, *see Illinois v. Rodriguez*, 497 U.S. 177, 188 (1990); *United States v. Kimoana*, 383 F.3d 1215, 1222 (10th Cir. 2004) (collecting cases), mandate that in consent-based, warrantless computer searches, law enforcement personnel inquire or otherwise check for the presence of password protection and, if a password is present, inquire about the consenter's knowledge of that password and joint

[4] The lead ICE agent testified that he did not believe sufficient evidence existed to obtain a search warrant. Given the evidence available to ICE in this case, acquired not only from initial records arising out of a large-scale, nationwide investigation but also subsequent investigation including surveillance and subpoenas for Defendant's records, I remain skeptical of ICE's belief that it lacked sufficient justification to obtain a search warrant. Nevertheless, the agent's opinion illustrates the apparent ambiguity presented by the circumstances of this case.

access to the computer.

This decision requires resolution of the voluntariness of Defendant's consent. In my mind, the critical inquiry is whether Defendant was in fact informed before giving consent that the officers had already examined his password-protected computer and found incriminating evidence. The district court failed to adequately resolve this dispute. It "note[d] for the record" the contradictory testimony, "considered the contradictions," and found that "the agents fully advised [Defendant] of the *circumstances* facing him." (Suppression Hr'g Tr. at 171 (emphasis added).) Absent further consideration and elaboration regarding exactly what facts comprised those "circumstances," I cannot determine whether Defendant's consent was impermissibly tainted. I would, therefore, reverse the district court's ruling on the issue of apparent authority and remand for further consideration of the voluntariness of Defendant's consent.