

**06-3094**

IN THE UNITED STATES COURT OF APPEALS  
TENTH CIRCUIT

UNITED STATES OF AMERICA,  
Plaintiff/Appellee,

v.

RAY ANDRUS,  
Defendant/Appellant,

On Appeal from the United States District Court  
for the District of Kansas

The Honorable Carlos Murguia  
U.S. District Judge

**BRIEF OF AMICI CURIAE  
COMPUTER FORENSICS RESEARCHERS AND SCIENTISTS  
IN SUPPORT OF APPELLANT AND  
REVERSAL OF THE DENIAL OF THE MOTION TO SUPPRESS**

PAUL OHM  
Associate Professor  
University of Colorado Law  
School  
401 UCB  
Boulder, Colorado 80304  
(303) 492-0384

JENNIFER GRANICK  
Executive Director  
Center for Internet and Society  
Stanford Law School  
559 Nathan Abbott Way  
Stanford, CA 94305  
(650) 724-0014

*ATTORNEYS FOR AMICI CURIAE*

**TABLE OF CONTENTS**

	<i>Page</i>
STATEMENT OF IDENTITY OF AMICI CURIAE, INTEREST IN THE CASE, AND SOURCE OF AUTHORITY TO FILE .....	1
ARGUMENT .....	4
INTRODUCTION .....	4
I. WHETHER AN INDIVIDUAL HAS LOCKED A CONTAINER IS A CRITICAL CONSTITUTIONAL FACT RELEVANT TO DETERMINING EXPECTATION OF PRIVACY, THIRD PARTY AUTHORITY TO CONSENT AND SCOPE OF CONSENT .....	5
II. PASSWORDS, LIKE LOCKS, ARE ONE OF THE MOST COMMON AND IMPORTANT WAYS TO SECURE COMPUTER FILES FROM OUTSIDERS AND THEIR “VISIBILITY” IS IRRELEVANT TO THE QUESTION OF WHETHER THEY IMPOSE PRACTICAL AND LEGAL LIMITS ON LAW ENFORCEMENT INVASIONS OF CONSTITUTIONALLY PROTECTED PRIVACY. ....	11
III. THE BURDEN ON OFFICERS TO CHECK FOR VIRTUAL LOCKS IS MINIMAL .....	19
CONCLUSION .....	27
CERTIFICATE OF COMPLIANCE	

## TABLE OF AUTHORITIES

### FEDERAL CASES

<i>Florida v. Jimeno</i> , 500 U.S. 248 (1991) .....	6, 9, 10
<i>Georgia v. Randolph</i> , 547 U.S. 103, 126 S. Ct. 1515 (2006).....	8
<i>Gillard v. Schmidt</i> , 579 F.2d 825 (3d Cir. 1978).....	7
<i>Illinois v. Rodriguez</i> , 497 U.S. 177 (1990) .....	6
<i>Kyllo v. United States</i> , 533 U.S. 27 (2001).....	5, 6, 7
<i>Schowengerdt v. General Dynamics Corp.</i> , 823 F.2d 1328 (9th Cir. 1987) .....	7
<i>Trulock v. Freeh</i> , 275 F.3d 391 (4th Cir. 2001).....	2
<i>United States v. Andrus</i> , 483 F.3d 711 (10th Cir. April 25, 2007) .....	2, 7, 8, 12
<i>United States v. Block</i> , 590 F.2d, 535 (4th Cir. 1978).....	3, 8
<i>United States v. Buckner</i> , 473 F.3d 551 (4th Cir. 2007).....	18
<i>United States v. Chadwick</i> , 433 U.S. 1 (1977) .....	6
<i>United States v. DeWeese</i> , 632 F.2d 1267 (5th Cir.1980) .....	7
<i>United States v. Ferrer-Montoya</i> , 483 F.3d 565, 568-69 (8th Cir. 2007) .....	11
<i>United States v. Fiorillo</i> , 186 F.3d 1136 (9th Cir. 1999).....	9
<i>United States v. Kinney</i> , 953 F.2d 863 (4th Cir. 1992).....	9
<i>United States v. Martinez</i> , 949 F.2d 1119 (11th Cir. 1992).....	11
<i>United States v. Matlock</i> , 415 U.S. 164 (1974) .....	6

<i>United States v. Milian-Rodriguez</i> , 759 F.2d 1558 (11th Cir. 1985) .....	11
<i>United States v. Morgan</i> , 435 F.3d 660 (6th Cir. 2006) .....	2
<i>United States v. Osage</i> , 235 F.3d 518 (10th Cir. 2000).....	10
<i>United States v. Patacchia</i> , 602 F.2d 218 (9th Cir.1979), amended regarding other matters by 610 F.2d 648 (9th Cir. 1979) .....	10
<i>United States v. Pena</i> , 920 F.2d 1509 (10th Cir. 1990).....	10
<i>United States v. Presler</i> , 610 F.2d 1206 (4th Cir. 1979) .....	7, 8
<i>United States v. Rith</i> , 164 F.3d 1323 (10th Cir. 1999) .....	6
<i>United States v. Salinas-Cano</i> , 959 F.2d 861 (10th Cir. 1992) .....	7
<i>United States v. Speights</i> , 557 F.2d 362 (3d Cir. 1977).....	7
<i>United States v. Strickland</i> , 902 F.2d 937 (11th Cir. 1990).....	10
<i>United States v. Whitfield</i> , 939 F.2d 1071 (D.C. Cir. 1991).....	4, 5

**STATE CASES**

<i>State v. Wells</i> , 539 So. 2d 464.....	10
---	----

## **STATEMENT OF IDENTITY OF AMICI CURIAE, INTEREST IN THE CASE, AND SOURCE OF AUTHORITY TO FILE**

Amici Curiae are experts in the field of computer forensics and all have extensive training and experience with the computer forensics tool EnCase. Amici have a direct and vital interest in the issues presented in this Court based on their professional, academic, and personal interest in the proper and legal use of computer forensics technology, and the proper interpretation of the constraints the Fourth Amendment places on their chosen professions. In addition, Amici have identified a number of significant misunderstandings of computer forensic technology in the initial majority panel's decision. Amici believe this Court would benefit from an accurate understanding of the technology and related issues, and that this brief would be proper under Federal Rule of Appellate Procedure 29.

**Marcus K. Rogers** is the Chair of the Cyber Forensics Program in the Department of Computer & Information Technology at Purdue University. Dr. Rogers is a Professor of Computer & Information Technology and a Research Scientist at the Center for Education and Research in Information Assurance and Security (CERIAS). Dr. Rogers holds a Doctorate in Forensic Psychology and is a former Law Enforcement Officer (Canada) (Detective) in a Computer Crime Unit. He has 13 years of Law Enforcement experience. Dr. Rogers is the Chair of the Certification Committee for the Digital Forensics Certification Board at the

National Center for Forensic Science and the Chair of the Ethics Committee for the new American Academy of Forensic Sciences (AAFS) Digital and Multimedia Forensics section (to be recognized in 2008). Dr. Rogers is a voting member of the Scientific Working Group on Digital Evidence (SWGDE), the American Society for Testing and Materials (ASTM) International and a member of the DOJ's Electronic Crime Partnership Initiative (ECPI). Dr. Rogers has numerous publications in the area of digital evidence investigations and is the Editor-In-Chief of the Journal of Digital Forensic Practice. He is a Certified Information Systems Security Professional (CISSP) and a Certified Computer Crime Investigator – Advanced, by the High Tech Crimes Network. Dr. Rogers is also the International Chair of the Law Compliance and Investigation Domain of the Common Body of Knowledge. Dr. Rogers has taught basic and advanced digital evidence investigations to over 500 Law Enforcement Officers, and presented invited lectures and keynote addresses for various national and international conferences including the National Institute of Justice, the National White Collar Crime Center, Association for Computing Machinery (ACM), National Science Foundation (NSF), and the Department of National Defense (Canada).

**Hugh Tower-Pierce** currently leads the computer forensics and technical investigation capability at a Fortune 100 financial services company. Previously, he worked at the National Center for the Study of Counter-Terrorism and

CyberCrime. Mr. Tower-Pierce is a member of the FBI InfraGard partnership, as well as a past Chair of the Vermont State Technology Advisory Board. He holds the SANS Institute GIAC Certified Forensic Analyst (Gold) accreditation, is an ISC2 Certified Information Systems Security Professional (CISSP), and a Digital Evidence Lab Inspector for the American Society of Crime Laboratory Directors / Laboratory Accreditation Board. Mr. Tower-Pierce graduated from Dalhousie University in Halifax, Nova Scotia.

**Samuel Liles** is a member of the faculty at Purdue University Calumet within the Computer Information Technology Department. He is a forensic science researcher. Professor Liles is a member of the Association for Computing Machinery, and the Institute of Electrical and Electronics Engineers. He has previously worked for major telecommunications companies, computer companies, the department of defense and most recently NCR Corporation. He is a graduate of Colorado Technical University in Colorado Springs, Colorado.

**Carole Fennelly** is an information security professional with over 25 years of hands-on experience in the computing technology field. She is the author of numerous articles for IT World, SunWorld and Information Security Magazine. Ms. Fennelly has led numerous post-incident forensic analysis efforts, ranging from informal system reviews to forensic analysis in criminal investigations. She wrote an article for Information Security magazine titled "On Trial" (October,

2004) that detailed the process an organization would endure when prosecuting computer crime cases. She also created a 5-day Computer Forensics course for Sun Microsystems that describes the procedural and technical process of performing a forensic analysis on Solaris systems.

## **ARGUMENT**

### Introduction

It is unreasonable for law enforcement agents searching a computer with a third party's consent to use tools to bypass password protection and user profiles to view information that the third party has no authority to access. Courts considering the Fourth Amendment's protections have given heavy weight to whether an individual has locked a container or taken other steps to restrict access by outsiders in determining expectations of privacy, the ability of third parties to consent to searches, and the scope of consent. Requiring law enforcement agents to heed locks is critical to keeping searches within the bounds of the Fourth Amendment. There is no reason to give passwords—digital locks—less weight than physical locks, especially because the search of a computer is often more intrusive and invasive than the search of a closet or a footlocker.

Even if Dr. Andrus effectively consented to the search of Ray Andrus' computer, law enforcement agents broke through digital walls into areas of the computer that were off limits to Dr. Andrus. This practice violates the Fourth

Amendment.

The Supreme Court held in *Kyllo v. United States*, 533 U.S. 27 (2001) that law enforcement agents may not use specialized search tools that intrude into protected areas without authorization. After Dr. Andrus gave law enforcement agents permission to access Ray Andrus' computer, the agents used a specialized tool in a way that they knew could potentially intrude beyond the area over which Dr. Andrus had authority to consent to search. This was reckless and unreasonable. Using the very same tool, the agents could have performed a simple test for the existence of user profiles and passwords, which would have imposed almost no burden on them. It is as improper for law enforcement agents to use a tool in a way which ignores passwords and user profiles as it would be for investigators to get a parent's permission to search a house and then use x-ray goggles to peer into their adult children's locked closets and footlockers. Accordingly, the evidence in this case should be suppressed because the search violated the Fourth Amendment.

**I. WHETHER AN INDIVIDUAL HAS LOCKED A CONTAINER IS A CRITICAL CONSTITUTIONAL FACT RELEVANT TO DETERMINING EXPECTATION OF PRIVACY, THIRD PARTY AUTHORITY TO CONSENT AND SCOPE OF CONSENT**

When an individual locks a container, excluding third parties from accessing the container's interior, the lock both manifests the owner's expectation of privacy and imposes a practical and constitutional barrier to warrantless searches into the

locked space. Locks are relevant at almost every stage of the Fourth Amendment inquiry.

The Fourth Amendment prohibits unreasonable searches and seizures. A search occurs when government agents intrude upon a constitutionally protected area, defined as an area in which the individual has a reasonable expectation of privacy. *Kyllo v. United States*, 533 U.S. at 33. A search is presumptively unreasonable if the investigators have no warrant, although it may be justified under an exception to the warrant requirement. *Illinois v. Rodriguez*, 497 U.S. 177, 190 (1990). One exception is search with the consent of the owner of an item or of a third party with joint access to or control for most purposes over the thing to be searched. *United States v. Matlock*, 415 U.S. 164, 171 (1974); *United States v. Rith*, 164 F.3d 1323, 1329 (10<sup>th</sup> Cir. 1999). The scope of a consent search may not exceed what the consenting party has authorized. *Florida v. Jimeno*, 500 U.S. 248, 250-52 (1991).

Locks strongly support a finding that the property owner has a reasonable expectation of privacy in the thing to be searched, a finding that triggers Fourth Amendment protection. “By placing personal effects inside a double-locked footlocker, respondents manifested an expectation that the contents would remain free from public examination. No less than one who locks the doors of his home against intruders, one who safeguards his personal possessions in this manner is

due the protection of the Fourth Amendment Warrant Clause.” *United States v. Chadwick*, 433 U.S. 1, 11 (1977). *See also United States v. Salinas-Cano*, 959 F.2d 861, 864 (10th Cir. 1992) (referencing “the precautions taken by the owner to manifest his subjective expectation of privacy, for example locking the container”); *Schowengerdt v. General Dynamics Corp.*, 823 F.2d 1328, 1331, 1335 (9th Cir. 1987) (plaintiff had reasonable expectation of privacy in his locked desk and credenza absent notice that items could be searched); *United States v. DeWeese*, 632 F.2d 1267, 1271 (5th Cir.1980) (crew member had legitimate expectation of privacy in areas such as foot locker which were accessible to only one individual); *Gillard v. Schmidt*, 579 F.2d 825, 828 (3d Cir. 1978) (school guidance counselor charged with maintaining sensitive student records had reasonable expectation of privacy in his school desk); *United States v. Speights*, 557 F.2d 362, 363 (3d Cir. 1977) (police officer had reasonable expectation of privacy in his locker where no regulations or practices would have alerted him to expect non-consensual searches and which he secured with personal lock); *United States v. Presler*, 610 F.2d 1206, 1214 (4th Cir. 1979) (locking two briefcases and retaining either the key or the combination to the locks was an effective expression of the defendant's expectation of privacy). On this point, the appellate panel in this case agrees. *United States v. Andrus*, 483 F.3d 711, 718 (10th Cir. April 25, 2007) (“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.” (citations omitted)).

Locks are also critical in determining who is authorized to consent. Judges approving third-party consent searches often point to the failure of the defendant to use a lock to exclude others. For example, in dissent in *Georgia v. Randolph*, Chief Justice Roberts opined that defendants who want to keep control over their possessions should lock them up. “To the 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.” 547 U.S. 103, 126 S.Ct. 1515, 1535 (2006) (Roberts, C.J., dissenting) (italics in original).

Police are not entitled to rely on third-party consent to search a locked area when the third-party lacks a key. *See, e.g., United States v. Block*, 590 F.2d 535, 537 (4th Cir. 1978) (mother’s authority to allow search of house did not extend to 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”); *United States v. Presler*, 610 F.2d 1206, 1214 (4th Cir. 1979) (no reasonable person could believe that defendant's friend had authority to consent to the search of the defendant's two locked briefcases). If a third party consents to the search of a locked container and presents a key to law enforcement, and if circumstances

lead the officers reasonably to believe that the person has common authority or the right to access the container for most purposes, then the officers may proceed with the search. This is so, under the doctrine of apparent authority, even if the consenter stole the key or did not have actual authority to give permission for some other reason. *United States v. Kinney*, 953 F.2d 863, 866 (4th Cir. 1992) (girlfriend stole key to boyfriend's locked closet but police reasonably believed she had granted valid consent to the search so the evidence need not be suppressed); *United States v. Fiorillo*, 186 F.3d 1136, 1144 (9th Cir. 1999) (holding that consenting party had apparent authority to allow a search of a locked back room when there was no indication prior to the search that the room was leased, the consenting party gave a key to the officials, and there was no sign or other indication on the door to the leased room).

Locks also help define the proper scope of an authorized search. For example, the U.S. Supreme Court in *Florida v. Jimeno* held that “consent to search a vehicle may extend to closed containers found inside the vehicle”, 500 U.S. 248, 250 (1991), but that locked containers are likely not covered by consent to search. “It is very likely unreasonable to think that a suspect, by consenting to the search of his trunk, has agreed to the breaking open of a locked briefcase within the trunk.” *Id.* at 251-52. Locks and other barriers are factors defining the scope of consent. For example, in *Jimeno*, the search of a closed paper bag was within the

scope of consent to search a car for drugs because it was “objectively reasonable for the police to conclude that the general consent to search respondent's car included consent to search containers within that car which might bear drugs”. *Florida v. Jimeno*, 500 U.S. 248, 251 (1991). However, “[w]hen the police are relying upon consent to conduct a warrantless search, they have no more authority than that reasonably conferred by the terms of the consent. If that consent does not convey permission to break open a locked or sealed container, it is unreasonable for the police to do so unless the search can be justified on some other basis.” *State v. Wells*, 539 So. 2d 464, 467 (Fla. 1989). Similarly, this Court has held that opening sealed cans fell outside the scope of the consent granted to search luggage. *United States v. Osage*, 235 F.3d 518, 521 (10th Cir. 2000). Similarly, in *United States v. Patacchia*, the defendant's consent to search his vehicle did not include permission to search the locked trunk which defendant said “could not be opened”). 602 F.2d 218, 219 (9th Cir.1979), *amended regarding other matters by* 610 F.2d 648 (9th Cir. 1979). *See also United States v. Strickland*, 902 F.2d 937, 942 (11th Cir. 1990) (consent to search a car does not permit slashing of the spare tire).

Consent can sometimes justify warrantless searches of secured areas but only where the consenting party has given broad, unqualified, comprehensive consent that extends to those locked areas and, if the consenter is present during

the search, the consenter fails to object to the officers' entry. *See, e.g. United States v. Pena*, 920 F.2d 1509 (10th Cir. 1990) (partial dismantling of side panels of car permissible in consent search); *United States v. Martinez*, 949 F.2d 1119 (11th Cir. 1992) (blanket consent to search warehouse unit included consent to search locked trunk of car in that unit, even though cops had to pry it open); *United States v. Milian-Rodriguez*, 759 F.2d 1558 (11th Cir. 1985) (defendant consented to search and volunteered that key to locked closet was in his briefcase off-site, police did not err in picking lock on closet door); *United States v. Ferrer-Montoya*, 483 F.3d 565, 568-69 (8th Cir. 2007): (unqualified consent to search vehicle for drugs includes consent to search any areas where drugs might be found).

In sum, Fourth Amendment limitations on government search and seizure turn significantly on whether the property owner used locks or otherwise took steps to exclude third parties. Ensuring that law enforcement officers respect locks is a fundamental part of ensuring that any government investigation complies with the Fourth Amendment and adequately protects constitutional privacy.

## **II. PASSWORDS, LIKE LOCKS, ARE ONE OF THE MOST COMMON AND IMPORTANT WAYS TO SECURE COMPUTER FILES FROM OUTSIDERS AND THEIR "VISIBILITY" IS IRRELEVANT TO THE QUESTION OF WHETHER THEY IMPOSE PRACTICAL AND LEGAL LIMITS ON LAW ENFORCEMENT INVASIONS OF CONSTITUTIONALLY PROTECTED PRIVACY**

Passwords are the critical, and sometimes only, way individuals can secure their most intimately private digital information from intruders, family members,

roommates and warrantless government intrusion. These digital locks are far more than mere visual indicators of a manifestation of intent to exclude others. *Cf. Andrus*, 483 F.3d at 717 (discussing “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”).

It is common practice for computer users, even when they are the sole users of a computer, to require a password to access the machine. It is also common for multiple users of a single machine to have separate accounts and profiles on their home computers. For example, the Microsoft Windows family of operating systems constitutes the vast majority of installed operating systems today. *See* <http://marketshare.hitslink.com/report.aspx?qprid=5>. Windows 95 and 98, which as their names indicate were released more than nine years ago, allow for separate user accounts and passwords which allow each user to set private, personal preferences. Windows XP (released in 2001) and Windows Vista (2006) also provide separate user accounts for each user, although these allow a user not only to manifest her expectation of privacy, but also to block other users from accessing her files. *See* Windows User Manuals, *available at* <http://www.microsoft.com/windowsxp/using/setup/winxp/accounts.mspx>, <http://windowshelp.microsoft.com/Windows/en-US/Help/5d82b9b6-0a55-4199-b5d1-5b25b6b106cb1033.mspx>; *see also* [EnCase Computer Forensics, The](#)

Official EnCE: EnCase Certified Examiner Study Guide (March 2006), p. 391

(“Windows NT, 2000, XP and 2003 create a series of files that are *unique* to each user. ...The first time a user logs onto one of these systems, a root user folder is created bearing the user’s logon name. Nearly all data unique to that user is *segregated* and *secured* in these folders” (emphasis added).)

Every other operating system with a more-than-minimal share of the installed-base today—Mac OS X, Unix, and Linux—also allow for passwords and user profiles. Every single operating system mentioned above either installs passwords by default or strongly encourages users to enable passwords during installation to protect privacy and security. Studies show that these operating systems account for more than 95% of today's installed user base. *See, e.g.,* Net Applications, *Operating System Market Share for April 2007*, <http://marketshare.hitslink.com/report.aspx?qprid=2> (reporting results of survey of operating systems as self-reported to web servers as 82.65% Windows XP, 4.42% Windows 2000, 3.89% Mac OS, 3.02% Windows Vista, 2.32% MacIntel, 0.8% for Linux, and 0.79% for Windows NT); Institute for Security Technology Studies, *Law Enforcement Tools and Technologies for Investigating Cyber Attacks: A National Needs Assessment* (2002), <http://www.ists.dartmouth.edu/TAG/lena.htm>.

Given the ubiquity of computers running operating systems capable of user passwords and profiles, many computers in use today are either locked to restrict

access to one and only one person (as was the case with Ray Andrus' computer) or separated into multiple private locked areas each accessible only by a particular user, like a single apartment building is separated into private apartments.

The widespread use of passwords matters for the Fourth Amendment because many cases have recognized that passwords serve the same role as physical locks, manifesting an expectation of privacy and excluding third parties. Third parties lack mutual use or control over password protected files and folders when they lack the password. *Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001) (co-user of computer had authority to consent to search of computer, but not to consent to search of defendant's password protected files) ; *United States v. Morgan*, 435 F.3d 660, 663 (6th Cir. 2006) (fact that wife and her husband did not have individual usernames and passwords for computer located in a common area was an important factor weighing in favor of her apparent authority to consent to the search of the machine); The *Andrus* majority agrees with this fundamental holding. *Andrus*, 483 F.3d at 719.

Nevertheless, the majority found apparent authority based on the assertion that a digital lock is different from other locks because it is hard to see. *Id.* at 718. ("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.”) It is irrelevant whether a password can be visibly “seen” by someone looking at a computer that is switched off. In the physical world, locks are also often invisible, but respected. Many door locks, as a prime example, are invisible. An officer often cannot tell whether a door has a locking mechanism merely by looking at the doorknob. The same is true for locks on cabinet doors, medicine cabinets, and many suitcases, none of which reveal “a locking device” on visual inspection.

In fact, even doors with visible locking devices often fail to reveal to the mere viewer whether they have been set in the lock position. Locks with visible locking mechanisms such as combination suitcase locks, many automobile doors, and wall safes reveal only the possibility of a locked container, but determining that they are locked requires more than mere visual inspection. In the world of physical locks, padlocks are an anomaly: the rare type of lock that is both visible and that one can conclude is locked using sight alone; but padlocks are not the only locks entitled to Fourth Amendment protection.

Rather than rely on vision alone, the police *test* physical containers to see if they are locked by trying to open them. Even with Dr. Andrus’ consent to search the house, if the police had jiggled Ray Andrus’ bedroom doorknob and had discovered it to be locked, the police would not have been allowed to enter the room unless the father had a key. *United States v. Block*, 590 F.2d, 535, 541 (4th

Cir. 1978). This would be true even if the door lacked a visible locking device. The search probably would have been immediately halted for three different doctrinal reasons: first, Ray Andrus would have been manifesting his expectation of privacy in his bedroom. Second, the locked door would have signaled a limit to Dr. Andrus' authority to consent, which would have obligated the police to ask him at least one more question, "do you have the key?" *See, e.g., United States v. Whitfield*, 939 F.2d 1071, 1075 (D.C. Cir. 1991) (holding " cursory questioning" of suspect's mother insufficient to establish right to consent to search of 29-year-old son's room). Finally, if police bypassed the locked door either by picking the lock, kicking down the door, or wheeling in an x-ray machine or thermal imager, they would have exceeded the scope of Dr. Andrus' consent to search.

Physical reality forces the police to check whether something is locked, either verbally, by questioning the third-party consenter, or physically, by pulling on the doorknob or container lid. The protections of the Fourth Amendment turn on basic facts about the way locks hold things shut in the physical world. Police should not be allowed to circumvent this protection simply because new technology enables the search of digital spaces without first testing for locks.

In fact, the U.S. Department of Justice recognizes the importance of user names and passwords in conducting computer forensic investigations. The DOJ's manual for law enforcement instructs examiners to "conduct a thorough

assessment by reviewing the search warrant or other legal authorization” and to determine case information such as “...passwords [and] user names” prior to acquiring the computer evidence. *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*, U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, pp. 7-8. Published April 2004. Available at <http://www.ncjrs.gov/pdffiles1/nij/199408.pdf>. The manual also instructs examiners to retrieve information about passwords. *Id.* at 12, 16-18. Prosecutors often want password information because the existence of password protection indicates ownership of the suspect files. *Id.* at 18. Despite the DOJ’s best practices, the investigators apparently chose to ignore the critical question of password protection in both the initial interview with Dr. Andrus and the forensic review of the computer files.

The majority holds that computer locks provide less constitutional protection than physical locks because police have forensic software that can bypass them. Rather than have to jiggle the knob or tug on the lid, computer investigators are able to look right through digital walls with EnCase. What the majority misunderstands is that practically all forensic software programs, including EnCase, are capable of checking to see whether files are password protected. Furthermore, EnCase is flexibly customizable and could be easily designed to check automatically for passwords and user profiles if law enforcement customers

had any interest in doing so. The Fourth Circuit considered exactly this problem in *United States v. Buckner*, 473 F.3d 551 (4th Cir. 2007). In *Buckner*, the defendant's wife did not have actual authority to consent to search of password-protected files but the court allowed the search pursuant to her apparent authority because nothing indicated to police that files were password protected. *Buckner* recognized, however, that officers could not “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.” *Id.* at 555, n. 3. Yet, the *Buckner* court, like the majority here, erred in holding that the police had no way of knowing that the defendant had a user account that excluded the consenting party. In fact, EnCase is a specialized tool the police are using in a willfully password-ignorant manner to get them past a technological and legal barrier they would not otherwise be able to or entitled to cross.

The United States Supreme Court has expressly disavowed the use of new technologies to circumvent traditional legal protections of private spaces. *Kyllo v. United States*, 533 U.S. 27 (2001). In *Kyllo*, police located in a public space used a thermal imaging device to monitor heat radiation from a private home. The Court held that even when law enforcement is legitimately present in the area from which it is doing a search, it may not use specialized search tools that intrude into constitutionally protected areas without authorization. “[o]btaining by sense-

enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical ‘intrusion into a constitutionally protected area,’ constitutes a search -- at least where . . . the technology in question is not in general public use.” *Id.* at 34 (citation omitted). According to *Kyllo*, it is the courts’ role to police citizen privacy in the face of technological change. The *Kyllo* opinion defines “what limits there are upon this power of technology to shrink the realm of guaranteed privacy.” *Id.*

The Fourth Amendment does not allow the government to ignore the walls of a home simply because police have a new technology that uses heat waves to perceive activities behind those walls. Nor does the Fourth Amendment allow the government to ignore locks, simply because the government has new technology that can bypass locks. In this case, EnCase gave the officers information they would have otherwise needed a warrant to obtain. As with the search in *Kyllo*, this search violated the Fourth Amendment.

### **III. THE BURDEN ON OFFICERS TO CHECK FOR VIRTUAL LOCKS IS MINIMAL**

In this case, the agents should have been required to check for virtual locks on Ray Andrus’ computer, to see if any attempt had been made to exclude others with passwords, thus establishing an expectation of privacy and limiting Dr. Andrus’ authority to consent and the scope of his consent. The police consciously

chose to disregard Ray Andrus' digital locks by using a forensic tool in a way that ignores user profiles and passwords. The forensic tool they used, EnCase, could have easily been used to respect and acknowledge user accounts and passwords. For purposes of the Fourth Amendment, the Court should recognize that law enforcement made a conscious choice to intentionally use EnCase in a manner that disregards passwords.

The majority decision rests on a false belief about user profiles, passwords, and tools like EnCase. The majority states, "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." *Andrus*, 483 F.3d at p. 719. This is incorrect, because agents can use EnCase to identify the presence of passwords and login screens without ever booting the machine. Furthermore, requiring police to make a check for digital locks in computer searches pursuant to third party consent would not pose a burden on investigators.

A typical computer stores data on a device called a hard drive. A hard drive is simply a sealed box containing metal platters on which are stored magnetic fields representing invisible bits of information. People rely on software to make the invisible bits appear as visible and concrete data. Ordinary users use operating systems like Windows XP to do this, and forensic examiners use tools like EnCase.

“Files” and “folders” are visible to forensic examiners only because EnCase interprets and repackages thousands or millions of bits of information into human-readable forms.

Other relevant information stored on a computer are (1) whether more than one user has ever accessed the computer; (2) whether access to the computer itself requires a password, and (3) whether specific files or folders are marked as private and off-limits to other computer users. EnCase provides easy access to all three of these types of information in its default configuration, although it is up to the human operator to bother to look at the information.

With absolutely no special configuration or modification, every version of EnCase we have used is capable of revealing quickly and simply how many user accounts are on the machine. First, in Windows XP (the version of Windows on Ray Andrus’ computer), the contents of the “Documents and Settings” folder can reveal whether the computer has been accessed by multiple user accounts. Clicking on this folder in EnCase reveals its subfolders, one folder for every user account on the machine, each bearing the name of a user account. *See [EnCase Computer Forensics, The Official EnCE: EnCase Certified Examiner Study Guide \(March 2006\), p. 363](#)* (“All versions of Windows NT (NT, 2000 XP, and 2003) create a unique artifact when the user first logs onto the system. A folder is created under Documents and Settings (200, XP, and 2003) or under Profiles (NT) that bears the

name of the logged-on user.”) If Agent Kanatzar had clicked on this folder during his on-site search, and the record indicates that he probably did, he would have immediately seen that this computer had been accessed via multiple usernames. Although this check would not have conclusively proved to Agent Kanatzar that Dr. Andrus lacked access to the files in Ray Andrus’ directory, to a trained forensics expert, this should have at least raised red flags about Ray Andrus’ attempts to exclude others from accessing his files, and about Dr. Andrus’ authority to consent to any search of the machine, never mind to search Ray Andrus’ personal user profile.

Furthermore, EnCase makes it possible to create a filter to exclude specified parts of the hard drive from review: a forensic technician merely needs to click on specific folders from among all of the folders on the hard disk to include them and only them in an operation. *See EnCase Computer Forensics, The Official EnCE: EnCase Certified Examiner Study Guide (March 2006), p. 440 et. seq.* (“Filters, Conditions and Queries”) Thus, in this case, Agent Kanatzar could have selected only shared directories and specific user profile directories during his search for images. It was not necessary to view images spread throughout the hard disk, including inside private user profiles.

Although the steps we have described thus far would be simple to perform for anybody with even a rudimentary understanding of EnCase, admittedly, they

would still require some, *minimal* human intervention (i.e., a few mouse clicks). Even this tiny amount of extra work would not be required if EnCase were configured automatically to perform a few quick user profile and password verifying steps. It would be trivial for the company that created EnCase, Guidance Software, or for any reasonably skilled EnCase user to program EnCase to expedite a check for digital locks on user accounts.

EnCase is highly configurable by its customers. For example, “EnScripts” are little pieces of software that can be “plugged into” EnCase to change the way EnCase operates. *See* [EnCase Computer Forensics, The Official EnCE: EnCase Certified Examiner Study Guide](#) (March 2006), p. 437-440 (“Running an EnScript ... is as simple as double-clicking on the EnScript name in the EnScript Tree Pane.”) Law enforcement agents typically use many EnScripts in their on-site and off-site forensic analyses, to allow them to use EnCase in automated and enhanced ways. For example, agents will often use an EnScript to perform what is called “signature analysis,” causing EnCase automatically to disregard files that are known to be irrelevant to the investigation. Many law enforcement EnCase experts develop and use their own EnScripts.

Although there are literally hundreds of ways we can imagine extending EnCase with EnScripts to make the program automatically reveal user profiles and login passwords, let us describe three. First, an EnScript could take advantage of

the meaning of the subfolders within the “Documents and Settings” folder, as described above, and alert the EnCase user with a pop-up screen that said, “this computer appears to have been accessed by different user profiles.” Second, an EnScript could do more than report the presence of separate user profiles, for example checking two important Windows databases (the SAM and Registry) to determine whether the computer is configured to display a login password prompt upon booting. Again, the presence or absence of a login prompt could be reported in a pop-up dialog box to the EnCase user at the start of the examination. Third, an EnScript could report the most recent login date and time for each user profile. Any of these three EnScripts would quickly perform their check and announce their results, telling the forensic examiner within seconds whether they could proceed with their consent search or whether further investigation might be required.<sup>1</sup>

EnCase could be made even more password and profile-aware. An EnScript could easily perform a “per file and folder” permissions check. So configured, whenever the forensic examiner selected any file or folder for display, EnCase could quickly check the “access control list” and display the names of the user accounts with permission to use or control that file or folder.<sup>2</sup> Again, the amount

---

<sup>1</sup> EnCase comes with a built-in example EnScript called “Sweep Case” which includes the ability to list information about every user on the computer.

<sup>2</sup> In fact, for well-trained EnCase users, this capability is available even without a

of time required to do this check would be practically unnoticeable.

A reasonably experienced EnCase user or Guidance Software employee could readily create any of these “consent search” EnScripts. *See, e.g.*, [http://www.guidancesoftware.com/products/ef\\_index.aspx](http://www.guidancesoftware.com/products/ef_index.aspx), (last visited May 25, 2007) (touting EnCase Forensics’ powerful scripting engine and an investigator’s ability to “save days, if not weeks, of analysis time by automating complex and routine tasks with prebuilt EnScript® modules, such as Initialized Case and Event Log analysis”.) EnCase has a built-in feature to allow automatic exclusion or inclusion of files and folders that a particular user has explicit permission to access. EnCase version 4 calls this the “Security ID Attributes” filter, which is available to all registered users of the software. This function may be augmented in later EnCase versions to allow searching as well as filtering. Thus, although EnCase provides its users the ability to check for digital locks manually and easily, it does not check for digital locks automatically, because Guidance Software does not configure it to work like that out of the box. This is likely because Guidance Software’s customer base, primarily law enforcement agencies and Fortune 1000

---

specialized EnScript. Investigators using EnCase in “preview mode” can manually view file permissions and access control lists. When highlighting a file or folder in EnCase, a small dot will appear in the “Permissions Column” whenever that file or folder has specific permissions associated with it. By then clicking “Details” in another part of the window, the examiner can list all the users that have access rights to the file or folder and what those rights are.

companies, have not asked for this feature.<sup>3</sup> This is no excuse. The police may want to search footlockers with x-ray machines, or homes with thermal imaging devices, but they cannot intentionally use tools in a way that purposefully ignore core, essential facts fundamental to their Fourth Amendment authority to search. Yet that is what law enforcement is doing, now with the blessing of the majority panel, despite how easily these agents could have performed a simple and quick check for digital locks.

We are not asking the Court to micromanage law enforcement computer forensics investigations. Obviously, technology experts should be given discretion to choose proper tools consistent with concerns of efficiency, evidence integrity (including chain of custody and admissibility concerns), and compliance with the law. But, as with the thermal imager in *Kyllo*, it is squarely within the courts' role to identify tools being used at odds with the Constitution. In *Kyllo*, the Supreme Court recognized that it is the responsibility of courts to define "what limits there are upon this power of technology to shrink the realm of guaranteed privacy." *Kyllo*, 533 U.S. at 34. As the dissent in this case so cogently notes, "[t]he unconstrained ability of law enforcement to use forensic software such as the EnCase program to bypass password protection without first determining whether

---

<sup>3</sup> Furthermore, the product is designed by former law enforcement officers. At the present time, six of the fourteen people on the executive team, have extensive law enforcement backgrounds.

such passwords have been enabled does not ‘exacerbate[]’ [the difficulty of ascertaining the existence of digital locks]; rather it avoids it altogether, simultaneously and dangerously sidestepping the Fourth Amendment in the process.” *Andrus*, 483 F.3d at 723 (McKay, J., dissenting). It is this Court’s responsibility to regulate the power of technology to shrink the realm of guaranteed privacy. We think that during a consent search of a shared computer, it is objectively unreasonable to use a tool in a way that intentionally disregards passwords.

## CONCLUSION

For these reasons, Amici support defendant Ray Andrus, reconsideration of the panel’s majority decision, and reversal of the ruling below.

Dated: May 31, 2007

Respectfully submitted,

---

JENNIFER GRANICK  
Center for Internet and Society  
Stanford Law School  
559 Nathan Abbott Way  
Stanford, CA 94305

PAUL OHM  
University of Colorado Law School  
401 UCB  
Boulder, Colorado 80304

*ATTORNEYS FOR AMICI CURIAE*

## **CERTIFICATE OF COMPLIANCE**

As required by Fed. Rules of App. Proc. 32 (a)(7)(C) I certify that this brief is proportionally spaced and contains 6,411 words.

I relied on my word processor to obtain the count and it is Word 2002.

I certify that the information on this form is true and correct to the best of my knowledge and belief formed after a reasonable inquiry.

---

Jennifer Granick  
*ATTORNEYS FOR AMICI CURIAE*

**CERTIFICATE OF SERVICE**

I hereby certify that on this 31st day of May, 2007, two (2) copies of the foregoing was sent via e-mail and Federal Express, to the following:

**BRIEF OF AMICI CURIAE  
COMPUTER FORENSICS RESEARCHERS AND SCIENTISTS  
IN SUPPORT OF APPELLANT AND  
REVERSAL OF THE DENIAL OF THE MOTION TO SUPPRESS**

David J. Phillips, Federal Public Defender  
Melissa Harrison #9705, Assistant Federal Public Defender  
for the District of Kansas  
500 State Avenue  
Kansas City, KS 66101-2400  
(913) 551-6712  
*Counsel for Appellant Ray Andrus*

Eric F. Melgren, United States Attorney  
District of Kansas  
Leon J. Patton, Assistant U.S. Attorney  
360 U.S. Courthouse  
500 State Avenue  
Kansas City, Kansas 66101  
913-551-6730  
*Attorney for Plaintiff/Appellee*

---

LYNDA JOHNSTON