INTRODUCTION

The Fourth Amendment preserves the “right of people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures.” A search by law enforcement pursuant to voluntary consent is a clearly recognized exception to the probable cause and warrant provision of the Fourth Amendment. “A search authorized by consent is wholly valid.” However, in order for such a search to be upheld, the consent must have been voluntarily given by one authorized to do so, and the search must not exceed the scope of the consent. Determining who is authorized to give consent to search a computer can be especially challenging in light of forensic software and other technological tools.

I. VOLUNTARY NATURE OF CONSENT

General Principle

Whether a search was voluntary or was the product of duress or coercion, either express or implied, is a question of fact that is determined by the totality of the circumstances, taking into consideration the characteristics of the defendant as well the facts surrounding the encounter with the officer. The government has the burden of proving consent by a preponderance of the evidence. It is interesting to note that while the Court discusses the characteristics of the person giving consent, in none of the Court’s decided cases has it held consent to be invalid due such a characteristic; the focus instead has been on whether there was coercion or assertion of authority by the government agent which in effect, vitiated the consent.

A. Characteristics of the person giving consent

- Knowledge of a right to refuse to consent to a search is not necessary in order for the search to be deemed voluntary; however it is a factor that may be considered.

- Age, education level, gender and race of the subject are all factors to be considered in the voluntariness equation. The absence of a high school degree does not automatically render a defendant’s consent invalid. Likewise, the fact

3 E.g., Matlock, 415 U.S. at 177; Schneckloth, 412 U.S. at 222.
5 Schneckloth, 412 U.S. at 234.
6 Mendenhall, 446 U.S. at 558, (citing Schneckloth, 412 U.S. at 226).
that a defendant is well-educated and intelligent does not necessarily mean he is not susceptible to coercion or manipulation by the police. 7

- A defendant’s prior experience with the law as well as the existence of mental deficiencies could be factors weighed in the determination as to whether consent was voluntary. 8

- A suspect’s ability to understand English may also be a consideration in certain cases. The burden upon the government to prove that consent was voluntarily given is heavier where it appears the person is unable to speak or readily understand the English language. 9

- The fact that consent was obtained by a suspect who was mentally agitated or under the influence of drugs or alcohol does not render consent involuntary. The question is whether the suspect possessed an awareness of what he was doing and was able to appreciate the nature and significance of his actions. 10

B. Acts of Government agent -

For the most part, the courts’ analysis of defendants’ character traits has been limited to an acknowledgment that they are a factor in the determination of voluntariness. And while the Court in Schneckloth listed various subjective factors relating to defendant’s mental state or character that might vitiate consent, courts rarely engage in any meaningful analysis of these factors. By and large, courts are willing to find that, at least in the absence of egregious police misconduct or coercion, consent by a suspect was voluntarily given. 11 It is a well settled principle that where there is coercion, there cannot be consent. 12

- Assertion of lawful authority -
  - Consent given after officer falsely states that he has a search warrant is not valid, as it is tantamount to telling the subject that he has no choice but to consent. 13 Some cases support the principle that officers may inform the subject of their intent to obtain a search warrant without vitiating the validity of a subsequent consent search, as long as their intent to do so is

---

7 State v. Raibley, 788 N.E. 2d 1221 (Ill. 2003) (well educated defendant’s degree in specialized field of aquatic biology did not necessarily equip him for police encounter).
9 United States v. Sanchez, 32 F.3d 1330 (8th Cir. 1994) (consent valid even though defendant spoke only Spanish and police spoke only English; officer communicated with defendant through bilingual codefendant passenger); Kovach v. U.S., 53 F.2d 639 (6th Cir. 1931); People v. Sesmus, 591 N.E.2d 918 (Ill. 1992) (although suspect alleged difficulty understanding English, court found that consent was valid; at trial she was able to read consent form she had signed); United States v. Wai Lau, 215 F. Supp 684, 686 (S.D.N.Y. 1963).
10 United States v. Rambo, 789 F.2d 1289, 1297 (8th Cir. 1986).
genuine. Police may not use a threat to obtain a warrant when there are no grounds to do so in order to induce submission.\textsuperscript{14}

- Consent to search is involuntary if the police, through deceit or misrepresentation, lead the suspect to believe that the request must be granted.

- Government must establish that defendant’s consent was unequivocally, specifically, and intelligently given. While characteristics of the defendant (age, intelligence, and education) indicated ability to consent, his statement to police that “You’ve got the badge, I guess you can” conveyed the belief that he had no choice but to give consent to the search.\textsuperscript{15}

- **Show of Force** - There is no bright line rule as to what type of police conduct renders consent involuntary.
  - The fact that several officers restrained a suspect at gunpoint, while indicative of coercion, did not invalidate consent, since police conduct was viewed in light of other circumstances, such as defendant’s sophistication and knowledge of the criminal justice system.\textsuperscript{16}

  - Defendant’s consent was not voluntary as it was given after eleven police, with guns drawn, arrested him at his apartment at five a.m. Defendant was in handcuffs and police were rounding up his fiancé and their two children.\textsuperscript{17}

- **Threats against relatives**
  - Consent not voluntary when given by a defendant who had been arrested, taken to jail and told by police that his girl friend would be arrested if he did not sign the consent form.\textsuperscript{18}

  - Courts have been willing to find that consent is not voluntary when police tell suspect they will have his or her child taken away unless consent is granted.\textsuperscript{19}

\textsuperscript{14} United States v. Evans, 27 F.3d 1219, 1231 (7th Cir. 1994).
\textsuperscript{15} United States v. Worley, 193 F.3d 380, 386 (6th Cir. 1999).
\textsuperscript{18} United States v. Bolin, 514 F.2d 554, 560-61 (7th Cir. 1975).
C. Nonverbal Conduct as Consent

Courts have recognized that a person’s non-verbal conduct can constitute consent to search.\(^\text{20}\) Gestures are often ambiguous, and in order to avoid unpredictable interpretation\(^\text{21}\) the intent of the defendant should be unmistakably clear.\(^\text{22}\)

- The government has the burden of proving that consent was voluntarily given
- Although a defendant initially refuses to consent, his subsequent or contemporaneous actions may constitute consent.\(^\text{23}\)
- Handing over car keys in response to officers request to search trunk,\(^\text{24}\) gesturing for officers to enter while stepping away from entry way,\(^\text{25}\) and motioning for police to follow consenter to another room\(^\text{26}\) are situations in which nonverbal conduct constituted consent.

II. SCOPE OF CONSENT

A. Limited by the Terms of Authorization

The Fourth Amendment requires that the scope of every authorized search be particularly described. The scope of a consensual search is generally defined by its expressed object. While the scope of a search pursuant to a search warrant is determined by the issuing magistrate and described in the warrant, the scope of a consent search is determined by the party permitting the search and described by the exchange between the party giving consent and law enforcement.\(^\text{27}\)

B. Objectively Reasonable

The standard for measuring the scope of a suspect’s consent is that of objective reasonableness; what would a reasonable person have understood by the exchange between the officer and the suspect? The government has the burden of proof to show that

---

\(^{20}\) United States v. Jones, 254 F.3d 692, 695 (8th Cir. 2001); United States v. Benitez, 899 F.2d 995, 999 (10th Cir. 1990).

\(^{21}\) State v. Raibley, 788 N.E.2d 1212, 1230 (Ill. 2003) (state has burden of showing consent was voluntary; cannot carry that burden by proving defendant shrugged); State v. Harris, 642 A.2d 1242, 1246-47 (Del. Super. Ct. 1993) (shrug, without other indicators present, is not enough to show consent to search) but see United States v. Wilson, 895 F.2d 168, 172 (4th Cir. 1990) (defendant’s acts of shrugging shoulders and raising arms in response to police’s request for permission to pat him down constituted consent.)

\(^{22}\) State v. Anthony, 761 N.E.2d 1188 (Ill. 2001).

\(^{23}\) United States v. Flores, 48 F.3d 467, 468-69 (10th Cir. 1995).

\(^{24}\) United States v. White, 42 F.3d 457, 460 (8th Cir. 1994).

\(^{25}\) United States v. Rosario, 962 F.2d 733, 737 (7th Cir. 1992).

\(^{26}\) United States v. Walls, 225 F.3d 858 (7th Cir. 2000).

the search was within the scope of consent.\textsuperscript{28} Courts will examine various factors, such as the officer’s explanation of what, when, where and why search is being conducted; whether there were express limitations (verbal or by conduct) made by person giving consent to search, and whether any modifications of request or limitations were given as search progressed.

- Police officer who received consent from driver to search his car for drugs did not exceed the scope of the consent by looking into a brown paper bag located on the floorboard of the car. It was objectively reasonable for police to believe the consent of search extended to the bag: (1) suspect did not place any limitations on the scope of the search, (2) suspect was aware officer was searching for drugs; and (3) it was objectively reasonable for officer to think consent granted by suspect included consent to search closed containers within car that might contain drugs.\textsuperscript{29}

- A reasonable person assessing exchange between agent and person granting consent would conclude that consent extended to the computer; agents sought consent to search residence for explosives and evidence relating to explosives and bomb-making. Request that the computer be returned after the FBI made a copy of the hard drive may serve as an indication that search was within scope of consent; defendant did not express an objection to the removal or the copying of the hard drive.\textsuperscript{30} Furthermore, the court held that the revocation of consent, which occurred two months after consent was granted, did not operate retroactively to invalidate the agent’s actions. In effect, the court held that there was no expectation of privacy in the mirror image copy that the FBI had consent to obtain, and that the agent could continue to search this mirror image even after consent was revoked.\textsuperscript{31}

- It would be reasonable to assume that a computer science graduate student who gives officers consent to search his computer would understand that the search would involve more than a cursory look when he agreed to let the officers take his computer back to the FBI office for examination.\textsuperscript{32}

- Defendant consented to search of computer for evidence of stalking, but limited consent to the D: Drive, My Files directory, Creative Writing folder. Police exceeded scope of search when they opened and viewed contents of a folder labeled “Offshore,” believing it contained evidence of tax violations.\textsuperscript{33}

\textsuperscript{28} United States v. Freeman, 482 F.3d 829, 832 (5th Cir. 2007) (citing Florida v. Jimeno, 500 U.S. 248, 251 (1991)).
\textsuperscript{30} U.S. v. Megahed, 2009 WL 722481 (M.D. Fla.).
\textsuperscript{31} Id.
Police exceeded scope of consent to search apartment in relation to intruder’s assault on a neighbor when they accessed defendant’s computer files. It would be reasonable to understand police intended to search for physical evidence of assault.  

III. CONSENT BY THIRD PARTIES

GENERAL PRINCIPLE
It is well-settled that consent to search, in the absence of a search warrant may, in some circumstances be given by a person other than the target of the search. The theories that allow searches based on third party consent are closely related: common authority and assumption of risk. In United States v. Matlock the Court defined common authority:

Common authority is ... not to be implied from mere property interest a third party has in the property. The authority which justifies third-party consent does not rest upon the law of property, with its attendant historical and legal refinements, but rests rather on mutual use of the property by persons generally having joint access or control for most purposes, so that it is reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit the common area to be searched.

The Fourth Amendment not only guarantees freedom from unreasonable searches, thus protecting against unreasonable government intrusions upon privacy, but also freedom from unreasonable seizures. The Fourth Amendment protects against unreasonable governmental interference into the possessor interests in property; this right against unreasonable deprivation of property is not inferior to the right to privacy. The rationale behind third party consent to search is based upon the diminished expectation of privacy in shared property; there is no similar diminished expectation of possession. One who shares access or control with another does not assume that this third party will exclude him from possession. Just as a third party cannot exclude the owner from his property, he cannot permit others to deprive the owner of his property by consenting to a seizure.

In analyzing the issue of third party consent, the Court has recognized two categories: actual authority to consent and apparent authority to consent.

34 United States v. Turner, 169 F.3d 84, 89 (1st Cir. 1999).
36 Matlock, 415 U.S. at 171 n.7.
A. Actual Authority

In the context of computer searches, third party consent issues commonly arise in cases involving employers, parents, spouses, and room-mates.

- Parents
  In the overwhelming majority of cases, courts are willing to find that consent by a parent is effective against a child living in the parent’s home. Minors are traditionally subject to the authority of their parents, regardless as to whether that authority is derived from their status as head of the household, a natural function of their parental authority, or as a cotenant of jointly occupied property.37

- Children
  An overwhelming majority of jurisdictions which have considered the issue have chosen not to create a *per se* rule that all minors lack the authority to consent to a search.38 Instead, the courts will typically look to the totality of circumstances when making a determination as to whether a minor had the requisite authority to consent, with age being one of the factors considered.39

Montana is the only state that categorically rejects the theory that a youth can provide legal consent to a search.40 The court in *State v. Schwarz*41 concluded that due to Montana’s enhanced right to privacy under Article II, Section 10, consent, as an exception to the warrant requirement must be narrowly construed, and as such, a youth under the age of sixteen does not have the authority to waive her parents’ privacy rights.42

- Employers
  - Governmental Employer
    Government employees may have a reasonable expectation of privacy in their offices or parts of their offices.43

---


41 State v. Schwarz, 136 P.3d 989, 992 (Mont. 2006).

42 Id. At 992.

Whether a government employee has a reasonable expectation of privacy in his workplace computer (and thus standing to challenge its search) is determined on a case-by-case basis.44

» Employee control over premises or property - The fact that an employee has exclusive use of a computer in his private office can indicate a legitimate expectation of privacy.45 The use of a computer password and lock on office door can further bolster this finding.46 Conversely, in Voyles v. State,47 the court held that a teacher had no reasonable expectation of privacy in the school district owned computer located on the teacher’s desk, where the desk was in the computer laboratory, and the computer was used in the course of instruction.48

» Policies, procedures and notice - If government employer does not notify employees their computer usage will be monitored and there is no indication that employees have routine access to the computers of other employees, an employee may have a reasonable expectation of privacy in his office computer.49 In Leventhal v. Knapek,50 the court held that Leventhal had a reasonable expectation of privacy in a computer located in his private office, even though technical support staff had access to all computers. The court noted that computer maintenance was normally announced; unannounced access had occurred only once and the intrusion had been minimal.51 Employers can likewise diminish or frustrate an expectation of privacy through policies, procedures, or notice. A policy that grants an employer the right to access all information stored on their computers can defeat any reasonable expectation of privacy an employee might have in files

44 Ortega, 480 U.S. 709.

45 Leventhal v. Knapek, 266 F.3d 64, 73 (2nd Cir.)


48 Id. at 306.

49 Slanina, 283 F.3d 670 (5th Cir. 2002).

50 Leventhal, 266 F.3d 64.

51 Id. at 73.
stored therein. \(^{52}\) Likewise, courts have found that employees do not have a reasonable expectation of privacy in files downloaded from Internet and stored on workplace computer in light of policies regarding Internet use that authorizes the employer to audit or monitor Internet use of its employees. \(^{53}\) A banner or screen that appears at every start up and gives notice to employees that computers could be monitored may eliminate an expectation of privacy \(^{54}\) but is not dispositive as to the issue. The actual practice and procedures of the employer are given due consideration. An expectation of privacy may exist in spite of such a computer banner if an employer allows its employees to use their computer for private communications, provides passwords to prevent others from accessing computers, and does not, in fact, monitor employees’ files. \(^{55}\)

- **Private Employer**
  A private employee may also have a reasonable expectation of privacy in his workplace computer. \(^{56}\) Courts generally employ an analysis similar to those in cases involving public employees. The use of a computer password and lock on office door can support a finding that an employee has a reasonable expectation in the context of his files. \(^{57}\) An expectation of privacy can be eliminated via a company’s policy requiring employees to consent to a search each time he used the company-issued computer. \(^{58}\)

- A finding that an employee has a reasonable expectation of privacy in his office or effects, including his computer, requires any search conducted by the government to comply with the Fourth Amendment’s reasonableness requirement. It is well-settled that permission to search may be obtained from a third party who possessed common authority over or other sufficient relationship to the premises or effects sought to be inspected. \(^{59}\) In essence, an employee can be said to assume the risk that another with

---


\(^{53}\) See United States v. Angevine, 281 F.3d 1130, 1134-35 (10th Cir. 2002); United States v. Simons, 206 F.3d 392, 398-99 (4th Cir. 2000).

\(^{54}\) Angevine, 281 F.3d 1130.


\(^{56}\) See, Ziegler, 474 F.3d 1184.

\(^{57}\) Ziegler, 474 F.3d at 1190.

\(^{58}\) Muick v. Glenayre Electronics, 280 F.3d 741 (7th Cir. 2002).

\(^{59}\) Matlock, 415 U.S. 164.
common authority over his computer (an employer) might permit the area to be searched.\textsuperscript{60}

The Court in \textit{U.S. v. Zeigler},\textsuperscript{61} found an employer to possess the requisite common authority over the defendant’s computer where the IT department had complete administrative access to the computer, the employer installed a firewall, and the employees were all told that computers would be monitored.\textsuperscript{62}

- Spouses

Generally, a spouse will have the actual authority to consent to a search of premises or property under the theories of common authority and assumption of risk as set forth in \textit{Matlock}.\textsuperscript{63} And while one spouse may not consent to a search of the personal effects of the other spouse if the consenting spouse lacks joint access or control, courts have routinely turned to the theory of apparent authority to uphold the validity of such searches.

\textbf{B. Apparent Authority}

\textbf{General Principle}

An officer may rely on the consent of a person who \textit{seems} authorized to consent, regardless of whether or not the person is actually authorized to give consent. The Supreme Court in \textit{Illinois v. Rodriguez},\textsuperscript{64} set forth an objective standard: would all of the facts available to the officer at the moment warrant a man of reasonable caution in the belief that the consenting party had authority over the premises?\textsuperscript{65} States may, however, depart on independent state grounds. For example, Montana’s State Constitution provides for an enhanced right to privacy\textsuperscript{66}, and for this reason, the Supreme Court of Montana rejected the \textit{Rodriguez} holding instead that third party consent is valid against a defendant only if the consenting party had the actual authority to grant consent.\textsuperscript{67}

\begin{itemize}
\item \textit{Id.} at 171; \textit{Ziegler}, 474 F.3d at 1191.
\item \textit{Zeigler}, 474 F.3d 1184.
\item \textit{Id.} at 1191-1192.
\item \textit{Matlock}, 415 U.S. 164.
\item MT. CONST. Art. 2, §§ 10, 11.
\item State v. McLees, 994 P.2d 683 (Mont. 2000).
\end{itemize}
- **Disagreement as to Granting Consent**

While it is true that consent to search may be given by one other than the target of the search, the issue becomes more complex when the interests of the parties authorized to give consent are divergent.

General Principle: In a 5-3 decision, the Supreme Court in *Georgia v. Randolph*\(^{68}\) held that a co-tenant’s consent does not suffice for a reasonable search if a potential defendant with self-interest in objecting is in fact physically present and objects.\(^{69}\)

- Justices Stevens, Ginsburg, Kennedy and Breyer joined Justice Souter’s majority opinion, with Justices Stevens and Breyer writing separate concurring opinions. Chief Justice Roberts wrote a dissent joined by Justice Scalia. In addition, Justices Scalia and Thomas wrote separate dissenting opinions. A reading of these decisions is akin to an exercise in legalistic volley ball, with each opinion seemingly aimed at undermining the analysis of the others.

- The Majority admitted it was drawing a fine line but reasoned that as long as there was no evidence that police removed the potentially objecting tenant from the premises to avoid a possible objection there is practical value in the clarity of complementary rules, one recognizing a co-tenant’s authority to grant permission when there is no fellow co-tenant on hand, and the other according dispositive weight to the fellow occupants contrary indication when he expresses it.\(^{70}\)

- In his dissent, Chief Justice Roberts classified *Randolph* as an assumption of the risk case and argued that one who shares information, papers or places with another assumes the risk that the other will in turn share this information with the government.\(^{71}\) Chief Justice Roberts also asserted that the Majority’s rule has no relationship to the privacy protected by the Fourth Amendment; instead it protects the co-owner who is lucky enough to be at the door when the police arrive, whereas a potentially objecting co-owner asleep in the next room, or who fails to come to the door for a host of other reasons loses out.\(^{72}\)

---

\(^{68}\) *Georgia v. Randolph*, 547 U.S. 103 (2006).

\(^{69}\) *Id.* at 122-23.

\(^{70}\) *Id.* at 136-37.

\(^{71}\) *Randolph*, 547 U.S. at 132-36.

\(^{72}\) *Id.* at 127, 136-37.
Effect of Defendant’s Prior Refusal

Although not uniformly resolved in case law, the issue as to whether a defendant’s prior refusal of consent invalidates the subsequent consent of a co-tenant seems to hinge on how literally a court interprets Randolph’s requirement that the defendant must be physically present.

- In United States v. Hudspeth, police uncovered child pornography while executing a valid warrant on defendant’s business computer. Police asked defendant for consent to search his home computer which he refused. The defendant was arrested and taken to jail. In the meantime, other officers went to the defendant’s home and asked defendant’s wife for permission to search the home computer, which she eventually granted. The Eighth Circuit noted that Randolph’s narrow holding referenced a defendant who was physically present, and therefore was not applicable. As such, defendant’s refusal to give consent did not invalidate the later consent granted by his wife - a cotenant possessing joint access or control over the computer for most purposes - and therefore authorized under Matlock.

- The Seventh Circuit in United States v. Henderson held that the objection of a physically present defendant was no longer effective once he was arrested and taken to jail, at which time an authorized third party could grant consent.

- The Ninth Circuit reached the opposite conclusion in United States v. Murphy, holding that “when a co-tenant objects to a search and another party with common authority subsequently gives consent to that search in the absence of the first cotenant the search is invalid as to the objecting cotenant.” The Court held that once a co-tenant refuses to grant consent, his objection remains effective until there is an objective manifestation that he has changed his position and no longer objects to the search.

---

73 United States v. Hudspeth, 518 F.3d 954 (8th Cir. 2008).
74 United States v. Henderson, 2008 WL 3009968 (7th Cir).
75 United States v. Murphy, 516 F.3d 1117 (9th Cir. 2008).
76 Murphy, 516 F.3d at 1124.
77 Id. at 1125.

Copyright 2009 © National Center for Justice and the Rule of Law
• **Effect of Defendant’s Removal by Police**

Cases not uniformly decided:

- In *United States v. Wilburn*, 78 police arrested defendant, placed him in a squad car in front of his apartment and then asked his live-in girlfriend for consent to search, which she granted. The Seventh Circuit held the consent was valid notwithstanding the fact that the defendant was never asked for, and therefore never refused, permission to search. 79

- However, there is case law that stands for the proposition that arrest and removal of a third party invalidates subsequent consent granted by an authorized third party. In *State v. Jackson*, 80 the court, while noting a lack of evidence that police removed defendant to avoid objection, found that this was the effect on potential defendant, and this effect on defendant was more important than the subjective intent of the officer. 81 In essence, the court classified the defendant as being physically present as required by *Randolph*, since but for the acts of the police, he would have remained at the scene. Therefore, his refusal to give consent invalidated the co-tenant’s consent.

### IV. APPARENT THIRD PARTY AUTHORITY TO CONSENT TO SEARCH COMPUTERS

Computers present unique Fourth Amendment challenges. Noting that computers are repositories for information, courts considering the issue of third party apparent authority to search computers have analogized computers to other types of containers, likening them to a suitcase or a briefcase. 82 However an analysis of Fourth Amendment issues regarding computers must necessarily be more nuanced than when considering an ordinary box due to the very nature of computers and the emergence of forensic software and other technological tools.

#### A. Password Protected Files

The inquiry whether the owner of a footlocker, suitcase, etc. has a subjective expectation of privacy in the contents located therein typically hinges on whether such container is

78 *Wilburn*, 473 F.3d 742 (7th Cir. 2007).

79 *Id.* at 745.


81 *Id.* at 466.

82 United States v. Andrus, 483 F.3d 711, 718 (10th Cir. 2007); Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir. 2001).
locked.\textsuperscript{83} The Fourth Circuit in \textit{United States v. Block}\textsuperscript{84} held that although a mother could consent to a search of her son’s room, the consent did not extend to a locked footlocker in which he expressed a subjective expectation of privacy.\textsuperscript{85}

It is not always readily apparent as to whether the owner of a computer has indicated a subjective expectation of privacy in his computer. The Court in \textit{Andrus} recognized this challenge:

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 a 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.”

\section*{B. Password-Circumventing Software}

- \textbf{Police Aware of Presence of Passwords}
  
  In \textit{Trulock v. Freeh},\textsuperscript{86} the Fourth Circuit analyzed whether the search of Trulock’s password-protected computer files, authorized by his housemate, was valid under the Fourth Amendment. The court found that Trulock’s use of a computer password was analogous to the use of the lock on a footlocker, and as in \textit{Block}, it shows he affirmatively intended to exclude his housemate from these files.\textsuperscript{87} The steps Trulock took to insure his files were inaccessible to his housemate (the creation of a password which he did not reveal) are evidence that he did not assume the risk that the files could be subjected to a search authorized by another. The court in \textit{Trulock} was not faced with the issue of apparent authority, in that the housemate informed police she did not know Trulock’s computer password.

\textsuperscript{83} \textit{Andrus}, 483 F.3d at 718 (citing United States v. Block, 590 F.2d 535 (4th Cir. 1978)).

\textsuperscript{84} \textit{Block}, 590 F.2d 535.

\textsuperscript{85} \textit{Id.} at 537.

\textsuperscript{86} \textit{Trulock}, 275 F.3d 391.

\textsuperscript{87} \textit{Trulock}, 275 F.3d at 403.

Copyright 2009 © National Center for Justice and the Rule of Law
Police Unaware of Presence of Password

Courts have upheld the validity of searches based on the consent of a third party even when the forensic software used to conduct the search revealed evidence in password-protected files.

- In United States v. Buckner, the Fourth Circuit upheld the validity of consent given by the defendant’s wife. She told officers she used the computer only occasionally to play solitaire. After shutting down computer, officers mirrored the hard drive and conducted a forensic analysis of the copy using software that did not reveal the husband’s files were password-protected. Court looked at totality of the circumstances available to the officer at the time of the search and concluded it was reasonable for police to think wife had authority.
  - computer located in common area;
  - computer was on / screen lit, even though husband not at home;
  - fraudulent acts committed came from that computer using accounts established in wife’s name;
  - computer leased solely in wife’s name;
  - officers had no indication files were password protected.

In dicta, the Court in Buckner said they were not holding that officers can rely on apparent authority to search while using technology to intentionally avoid the discovery of passwords or encryption put in place by the user.

- In Andrus, the Tenth Circuit also addressed the issue of the validity of a computer search authorized by a third party - the defendant’s 91 year old father with whom the defendant lived. However, in Andrus, the police were unaware of the presence of computer passwords because the party authorizing the search did not reveal this fact. The agents used a software program that copied Andrus’ hard drive without indicating whether any of the files were password protected.

The court noted that an officer presented with ambiguous facts relating to authority has a duty to investigate further before relying on consent.

88 United States v. Buckner, 473 F.3d 551 (4th Cir. 2007).
89 Buckner, 473 F.3d at 556, n.3.
90 Andrus, 483 F.3d 711.
91 Id. at 713-14.
92 Id. (quoting United States v. Kimoana, 383 F.3d 1215, 1222 (10th Cir. 2004)).
However, in analyzing the totality of the circumstances available to the officers, the court found they could have reasonably believed that the defendant’s father possessed mutual use or control over the computer and therefore authority to consent to the search. As a result, the officers were under no obligation to ask clarifying questions.93

» The one computer in the house was located in defendant’s room. The door was open, and the father said he was free to enter the room, but always knocked if the door was closed;
» The father owned the house and lived there;
» Father paid ISP bill; and
» Father did not say or do anything to indicate his lack of control over the computer at the time he was asked to give consent.

Likewise while refusing to take judicial notice that password-protection is a standard feature of operating systems, the Majority in Andrus did concede that if it is shown that there is a high incidence of password-protection among home computer users, the use of forensic software that bypasses passwords “may well be subject to question.”94

C. Password Circumventing Tools: The “Wink & Nod Approach to Third Party Authority?

Password circumventing software can be a valuable tool in enabling law enforcement officers who are equipped with a valid search warrant to expedite the time consuming process of searching a computer. But, the holdings set forth cases analyzing third party consent seem to lend credence to the proposition that an officer who either knows an suspect is not present and therefore cannot object, or has objected but was since arrested and taken to jail, may rely on the consent of a third party who seems to have a nexus to the computer. As long as the third party does not indicate the presence of passwords, the officer may use forensic software to search the computer and need not ask further questions. In effect, it will be as though the lock on the container (the password on the computer or computer file) did not exist at all.

It is understandable that one doing a forensic examination would not want to turn on a computer that is the target of the search - time and date stamps are altered, and booby traps could initiate a wiping process. These are just a few of the practical concerns. The use of forensic software that enables an investigator to make a copy of the computer without having to power up the machine can negate these potential issues.

91 Andrus, 483 F.3d at 720.
94 Id. at 722, n. 8.
But what about the fact that such software bypasses the protections put in place by the suspect? In *Kyllo v. United States*, 533 U.S. 27 (2001), the Supreme Court held that the Fourth Amendment doesn’t allow the government to ignore the walls of a home simply because the police have new technology that uses thermal imaging to perceive activities behind those walls. Should the Fourth Amendment allow the government to ignore computer locks in the form of passwords because the government has the technology to bypass them?

Returning to *Andrus* for a moment, assume that police want to search the son’s room in the house that Dr. Andrus owns. After obtaining consent from Dr. Andrus, would the police proceed to break down the door of the bedroom with a battering ram? Would they take the door off of the hinges? No, presumably they would first try the door knob, and if finding it locked, would ask Dr. Andrus if he has a key to his son’s room. If Dr. Andrus produces a key, the police may proceed with the search, secure in their knowledge that they are relying on the consent granted by an authorized party.

There are at least a couple of very simple practices that the police could employ that could help mitigate some of the problems arising from consent to search based on apparent third party authority. First, the police could simply ask the person granting consent general questions regarding his use of the computer, including whether he knew if the computer was password protected and if so, did he know the password? Another practice that the police could adopt would be to configure the forensic software to check for the presence of passwords. For example, EnCase, one of the premier tools used by law enforcement and forensic examiners is highly configurable by users and provides users with the ability to easily check for digital locks manually. Both of these low-tech practices could go a long way to ease the ambiguities in third party consent searches of computers as they could reveal not only the presence of a subjective expectation of privacy but perhaps a lack of authority to consent, as well.

---

37 *Id.*
38 State v. Lacey, 204 P.3d 1192, 1207 (Mont. 2009) (citing People v. Blair, 748 N.E. 2d 318 (Ill. App. Ct. 2001)).