2009

Apparent Authority in Computer Searches: Sidestepping the Fourth Amendment

John-Robert Skrabanek
University of Kentucky

Recommended Citation
Available at: https://uknowledge.uky.edu/klj/vol97/iss4/6

Follow this and additional works at: https://uknowledge.uky.edu/klj
Part of the Fourth Amendment Commons
Click here to let us know how access to this document benefits you.

This Note is brought to you for free and open access by the Law Journals at UKnowledge. It has been accepted for inclusion in Kentucky Law Journal by an authorized editor of UKnowledge. For more information, please contact UKnowledges@lsv.uky.edu.
Apparent Authority in Computer Searches: Sidestepping the Fourth Amendment

John-Robert Skrabanek

INTRODUCTION

In an era in which information storage is increasingly digitized, the computer password is king. As we undergo a massive transition away from paper records, more than anything else it is the password that will protect our most private files. This statement holds true for all types of data, from harmless personal digital photos to important state security documents. However, in contrast to the “brick and mortar” world, passwords in the digital context do not manifest themselves in tangible ways. For example, unlike a visible combination lock on a suitcase, frequently police may never know if a computer is password protected unless they make the effort to search for such protection. Should the legal standards that govern searches in this context be any different from those in a non-computer context? For a narrow subset of third-party consent searches, the answer is yes. Currently, the standards that control third-party consent searches in the area of digital storage are not adequate to protect the individual against unnecessary governmental intrusion.

This Note examines the search and seizure doctrine of “apparent authority” as applied to computer hard drives. Part I introduces the background and history of apparent authority in the “brick and mortar” world. Part II examines how the doctrine has narrowed over time to suit items that society considers especially private. Part III scrutinizes the current jurisprudence of apparent authority in the computer context, noting that authorities have frequently ignored or warped the proper inquiry that should be made in various situations. Part III also proposes that when searching hard drives, additional inquiries must be made by law enforcement officials before courts should allow these searches to pass constitutional scrutiny. Finally, Part IV offers other special considerations and issues regarding apparent authority in the context of computer searches.

---

1 B.A., 2005, Political Science, University of Kentucky; J.D. expected May 2009, University of Kentucky College of Law.
I. APPARENT AUTHORITY’S HISTORICAL ROOTS

A. Common Authority Beginnings

The Fourth Amendment to the United States Constitution generally provides the public the right to be free from unreasonable searches and seizures. Thus, warrantless searches are deemed "per se unreasonable" save for "exigent circumstances" or based upon a party's valid consent to a search. Any evidence obtained pursuant to a warrantless search is excluded at trial. Numerous exceptions arise, however, when law enforcement officials perform searches based upon an objectively reasonable but misinformed belief about a particular fact relating to their authority to conduct the search, resulting in some evidence found pursuant to a warrantless search admissible at trial.

For consent searches, the doctrine of "common authority" allows warrantless searches founded upon the consent of one party who possesses common control over property as against an absent, non-consenting party with whom that control is shared. First outlined in United States v. Matlock, the Supreme Court defined common authority not merely as based upon a property interest, but as requiring evidence of "mutual use" by one generally having "joint access or control for most purposes." If no mutual use is present, then there must be some form of assumption of the risk by the non-consenting party that a co-inhabitant would have the right to permit a search of a common area. It is always the government's burden to establish that common authority exists over the premises, and as with all consent searches, consent must be "freely and voluntarily given." Likewise, the scope of a consent search may not exceed what the consenting party has authorized. Finally, the standard for measuring the scope of the consent objectively asks what the typical reasonable person would have

---

2 U.S. CONST. amend. IV.
8 Id. at 171 n.7.
9 Id.
understood by the exchange with the officer. Considering the estimation that as many as 98% of all warrantless searches are conducted via some form of consent, the judicial creation, recognition, and enforcement of the common authority doctrine has a serious impact upon individuals' Fourth Amendment rights. Simply put, the validity of the particular third-party consent is critical to whether a great number of warrantless searches will withstand scrutiny in courts across the United States.

B. Expansion Into Apparent Authority

Following Matlock, in Illinois v. Rodriguez, the Supreme Court extended common authority further into an arena now deemed “apparent authority.” In Rodriguez, the defendant was suspected of drug possession and physical assault, but officers did not have a warrant to search his apartment. They conducted a warrantless search pursuant to the consent of a woman named Gail Fischer. Fischer represented that she shared the apartment with the defendant, had clothes and furniture inside, and unlocked the apartment door with a key. Fischer indicated several times that the apartment was “our[s]” (referring to herself and the defendant), but never clearly indicated whether she currently lived with the defendant or had only done so in the past. Based upon factual findings that Fischer had not lived with Rodriguez for over a month before the time of the search, had taken most of her household items with her in the move, had only occasionally frequented Rodriguez's apartment, and had never gone there by herself when he was not home, the Court found that the state had not carried its burden of showing that Fischer exhibited the adequate amount of common authority to uphold the search. Nevertheless, relying on past authority indicating police action generally only need be “reasonable” but not always “correct,” the Court excused the officers' mistakes and instead relied on their objective, good faith belief about the living situation. Ultimately, the Court held that a “warrantless entry is valid when based upon the consent of a third party whom the police, at the time of the entry, reasonably believe to possess common authority over the premises, but who in fact does not

13 Id. at 251.
14 1 Joshua Dressler, Understanding Criminal Procedure § 16.01, at 261 (4th ed. 2006) (estimated by one detective to be as high as 98%).
15 Rodriguez, 497 U.S. at 187.
16 Id. at 179–80.
17 Id.
18 Id. at 179.
19 Id. at 181–82.
20 Id. at 185.
21 Id. at 186.
do so." Therefore, actual authority is not necessary when the reasonable belief of apparent authority exists. Stated differently, courts only need to find either common authority or the reasonable belief of apparent authority for third-party consent searches to be valid.

While apparent authority expands the reaches of the power to conduct a warrantless search even further than common authority alone, several limiting factors prevent law enforcement from abusing apparent authority by conducting more warrantless consent-based searches than necessary. Foremost, the reasonableness of an officer's determination concerning the authority of a consenting party is judged by the facts available to the officer at the moment of the search. Furthermore, warrantless entry in light of an ambiguous situation is unlawful unless actual authority exists.

An example of this latter requirement can be found in the D.C. Circuit case of United States v. Whitfield. In Whitfield, the defendant was suspected of robbery, and his mother consented to a search of his room when he was not present. The search was originally upheld upon apparent authority grounds but was later overturned upon doubts as to whether the defendant was merely an occupant of his mother's house or in a landlord-tenant relationship with her (in which case she would not have had the authority to consent to such a search). The court of appeals stated unambiguously that the burden to prove the reasonableness of reliance upon apparent authority "cannot be met if agents, faced with an ambiguous situation, nevertheless proceed without making further inquiry." The court added that "if the agents do not learn enough, if the circumstances make it unclear whether the property about to be searched is subject to 'mutual use' by the person giving consent," then the police cannot constitutionally proceed with the search.

Another example of the duty to investigate ambiguous circumstances is found in United States v. Kimoana, where the Tenth Circuit Court of Appeals upheld the conviction of a felon for possessing firearms. In Kimoana, the defendant's friend consented to a search of a hotel room registered in the defendant's name, and the officer found a long-barreled revolver inside the room. Despite the fact that the defendant's attempt to suppress the evidence was ultimately denied, the court clearly stated that "where an

22 Id. at 179.
23 Id. at 188 (quoting Terry v. Ohio, 392 U.S. 1, 21-22 (1968)).
24 Rodriguez, 497 U.S. at 188-89.
26 Id. at 1073.
27 Id. at 1074-75.
28 Id. at 1075.
29 Id.
30 United States v. Kimoana, 383 F.3d 1215, 1219 (10th Cir. 2004).
31 Id. at 1220.
officer is presented with ambiguous facts related to authority, he or she has a duty to investigate further before relying on the consent."

Case history, then, makes it clear that apparent authority is a powerful tool used by law enforcement to legally conduct warrantless searches. The onus, however, is entirely on the state to conduct a reasonable inquiry into the nature of the apparent authority before proceeding, so as not to create the potential for abusive or haphazard searches.

II. THE NARROWING OF APPARENT AUTHORITY OVER TIME

Despite the generally broad power given by courts to police officers in reliance upon the apparent authority of third parties under Matlock and Rodriguez, the scope of the doctrine has narrowed significantly over time. In Stoner v. California, the Supreme Court warned that "[o]ur decisions make clear that the rights protected by the Fourth Amendment are not to be eroded by strained applications of the law of agency or by unrealistic doctrines of 'apparent authority.'" In Stoner, the search of an armed robbery suspect's hotel room without his consent was deemed unlawful even though it was conducted with the consent of a hotel employee. The Court opined that third-party consent, no matter how voluntarily and unambiguously given, cannot validate a warrantless search when the circumstances provide no basis for a reasonable belief that shared or exclusive authority to permit inspection exists in the third party giving consent.

Following Stoner's lead, courts across the country began to limit the ability of apparent authority to validate searches when the items being searched were considered more private. The seminal limiting case is United States v. Block, where a mother's consent to a search of her son's bedroom while he was not home was initially deemed valid based upon apparent authority, but such authority did not extend to the padlocked footlocker at the end of his bed. The officers began a search of the defendant's room and noted a lock on the trunk. They proceeded to ask the defendant's mother if she had a key to open it, and she indicated she did not. Nevertheless, the officers were able to open it with sheer blunt force. Fact-finding by the trial court indicated that the trunk "had been [the defendant's] private property over a period of around ten years; that during this time it was kept in his room, locked while he was away; and that neither his mother nor anyone else had

32 Id. at 1222 (emphasis added).
33 See also United States v. Rosario, 962 F.2d 733, 738 (7th Cir. 1992); Kaspar v. City of Hobbs, 90 F. Supp. 2d 1313, 1319 (D.N.M. 2000).
35 Id. at 487–88.
36 Id. at 489.
37 United States v. Block, 590 F.2d 535, 541 (4th Cir. 1978).
38 Id. at 537.
means of access to its interior nor permission to open it."

Invalidating the search, the court noted the extreme protection that should be accorded to our most private items, such as locked boxes:

Common experience of life . . . surely teaches all of us that the law's "enclosed spaces" mankind's valises, suitcases, footlockers, strong boxes, etc. are frequently the objects of his highest privacy expectations, and that the expectations may well be at their most intense when such effects are deposited temporarily or kept semi-permanently in public places or in places under the general control of another.

The 1984 Supreme Court case of United States v. Karo further extended the rationale of Block. In Karo, police were tracking the location of a beeper they had put in a large can of ether that was suspected of being used to make cocaine. The beeper was transported to a location owned by an individual not under investigation and with an individual privacy interest unique from the others under police surveillance. Justice O'Connor, in concurrence, agreed with the Court in upholding the search of the entire home, but only because the beeper pointed to the location of a more generalized area to be searched. In the alternative, she indicated that "[the] privacy interest in a home itself need not be coextensive with a privacy interest in the contents or movements of everything situated inside the home . . . . A homeowner's consent to a search of the home may not be effective consent to a search of a closed object inside the home." Supplementing this analysis, she specified that "when a guest in a private home has a private container to which the homeowner ... lacks the power to give effective consent to the search of the closed container."

In United States v. Salinas–Cano, the Tenth Circuit Court of Appeals followed the Supreme Court's indications from Karo by overturning a search of the defendant's suitcase that he had left at his girlfriend's apartment. The defendant was arrested after a controlled drug buy, but officers wanted to search his girlfriend's apartment for his possessions, admittedly having no probable cause to do so and with authority based only upon her valid consent. The apartment search was initially upheld on the rationale that because the girlfriend had control over the apartment, she had control of

39 Id. at 538.
40 Id. at 541.
42 Id. at 708.
43 Id. at 720.
44 Id. at 725 (O'Connor, J., concurring) (emphasis added).
45 Id. at 726.
47 Id. at 862.
everything in it and could consent to the search.\textsuperscript{48} Despite this holding, the court of appeals deemed the suitcase search unlawful because the girlfriend had neither actual nor apparent authority to consent to a search of her boyfriend's personal effects. The court indicated that the suitcase is an object long equated with a heightened expectation of privacy and that the searching officers were aware that the girlfriend had verbally discharged ownership of it.\textsuperscript{49} Furthermore, the court warned:

It is not enough for the officer to testify, as he did here, that he thought the consenting party had joint access and control. The "apparent authority" doctrine does not empower the police to legitimate a search merely by the incantation of the phrase. The Supreme Court's analysis of this subject instead rests entirely on the \textit{reasonableness} of the officer's belief.\textsuperscript{50}

Consequently, courts do not treat apparent authority as some sort of panacea that releases state agents from the obligation to conduct reasonable inquiries into the nature of third-party consent. To the contrary, \textit{Salinas-Caro} and \textit{Karo} represent the norm rather than the exception. Other examples of courts deeming searches invalid under an apparent authority analysis include the Ninth Circuit, where a suitcase was in the consenter's apartment;\textsuperscript{51} the Fifth Circuit, where cabinets were locked within the consenter's home;\textsuperscript{52} the D.C. Circuit, where a government employee's desk was located in the consenter's office;\textsuperscript{53} the Third Circuit, where a garage under the sole possession of a husband with one key was accessed under his wife's consent;\textsuperscript{54} and the Eastern District of Louisiana, where a closed overnight bag was found in the consenter's closet.\textsuperscript{55} Each of these cases demonstrates the limitation courts place on apparent authority in a context of anything less than shared ownership or with items normally associated with a heightened expectation of privacy. The more private that society generally considers the item to be searched, or the more obvious it is that the particular item only has one owner, the more likely courts are to be wary of searches premised exclusively upon apparent authority consent.

\textsuperscript{48} \textit{Id.}
\textsuperscript{49} \textit{Id.} at 865.
\textsuperscript{50} \textit{Id.} (citation omitted) (citing \textit{Illinois v. Rodriguez}, 497 U.S. 177, 183–89 (1990)).
\textsuperscript{51} \textit{United States v. Wilson}, 536 F.2d 883 (9th Cir. 1976).
\textsuperscript{52} \textit{Holzhey v. United States}, 223 F.2d 823 (5th Cir. 1955).
\textsuperscript{53} \textit{United States v. Blok}, 188 F.2d 1019 (D.C. Cir. 1951).
III. APPARENT AUTHORITY IN THE
COMPUTER SEARCH AND SEIZURE CONTEXT

A. Ignoring the Katz and Rodriguez Requirements

In 1967, Justice Harlan stated in his famous concurrence in the landmark case of *Katz v. United States* that a search violates the Fourth Amendment when the government violates a subjective expectation of privacy that society recognizes as reasonable.56 This hallmark of Fourth Amendment analysis is still adhered to in modern search and seizure jurisprudence. Thus, the first and most important inquiry that must be made as to the constitutionality of any search with a new technology is to what extent the subject exercised caution and care to keep the area private. In 2001, the Court extended the rationale of *Katz* in *Kyllo v. United States*, which held that the warrantless use of advanced technology to gather information regarding the interior of a home that could not otherwise have been obtained without physical intrusion is unconstitutional.57 Combined, these holdings establish a framework for any case involving a search that uses a new technology which the public has no knowledge of or for a search of a new physical area (ex. an entire computer hard drive).

The key questions under *Katz* and *Kyllo* that must be answered before a search can be upheld are to what extent the individual took steps to keep his possessions private and whether society recognizes this expectation of privacy as a reasonable one. Unfortunately, cases involving apparent authority searches of computer hard drives seem to circumvent these questions altogether by failing to establish whether or not the user had any password protections on the computer before initiating a search.58 In this line of cases, no question is ever posed as to what extent the individual intended to keep his files private. What is more, these cases also ignore the requirements from the *Rodriguez* progeny that officers conduct a reasonable inquiry into ambiguous cases, because if a user has password protected his computer or particular files, then obviously no common authority over that property can exist.

B. United States v. Buckner and United States v. Andrus
as the Incorrect Approach

There are a variety of examples of modern courts allowing officers to ignore the requirement that they make a reasonable inquiry into the circumstances of an ambiguous apparent authority situation. By allowing

58 See, e.g., *United States v. Buckner*, 473 F.3d 551 (4th Cir. 2007); *United States v. Andrus*, 483 F.3d 711 (10th Cir. 2007).
such searches, these courts have created the incentive for law enforcement 
\textit{not} to ask questions, an incentive contrary to the long line of cases following \textit{Rodriguez} and \textit{Stoner} that attempted to limit the power of apparent authority in unclear situations.\footnote{See supra Part II.}

The Fourth Circuit case of \textit{United States v. Buckner} provides an excellent example of a court creating such an incentive.\footnote{\textit{Buckner}, 473 F.3d at 551.} In \textit{Buckner}, Michelle Buckner was suspected of wire and mail fraud after authorities found multiple eBay accounts opened in her name.\footnote{Id. at 552.} She informed police that she knew nothing of such illegal transactions, and that while the computer was rented in her own name, the only reason she used it was to occasionally play solitaire.\footnote{Id. at 553.} When the defendant, her husband, was not present, she consented to a full search of the computer, telling officers "to take whatever [they] needed" and that she "want[ed] to be as cooperative as she could be."\footnote{Id.} Despite the fact that the computer was initially turned on at the time of the search, the officers shut it down and performed a "mirroring" procedure where they copied the entire contents of the hard drive; this procedure did not include restarting the computer or checking for any sort of password.\footnote{Id.} Later, the defendant attempted to have the evidence suppressed for lack of actual or apparent authority. At a suppression hearing, he testified that authentication \textit{was} in fact required to use the computer and that he was the only one who knew the password.\footnote{Id. at 554.} This testimony was accepted without contradiction, and officers admitted that they had made no further inquiries as to the ownership of the computer with the defendant’s wife, instead relying on the fact that the computer was leased in her name and located in a common living area of the home.\footnote{Id. at 555.}

In analyzing the validity of the search, the court agreed that Michelle had no \textit{actual} authority.\footnote{Id. at 554.} Here it relied on the rationale from \textit{Block} that, "[a]lthough common authority over a general area confers actual authority to consent to a search of that general area, it does not ‘automatically . . . extend to the interiors of every discrete enclosed space capable of search within the area.’"\footnote{Id. (quoting United States v. Block, 590 F.2d 535, 541 (4th Cir. 1978)).} Still, the court believed that apparent authority was reasonable under the circumstances, despite Michelle’s statements that she was “not computer-savvy” and that she used the computer solely to “play
The court did not discuss the lack of questions from the officers regarding Michelle’s ownership or use of the computer. However, the court erroneously attributed significance to the fact that while the search was taking place, “nothing the officers saw indicated that any computer files were encrypted or password-protected.” Rather, this should have been deemed irrelevant because it did not occur at the time of the initial inquiry. Officers are obligated to investigate any ambiguous situation of ownership before they begin a search, not during it. Case history further supports this view. According to the Sixth Circuit in United States v. Morgan, facts acquired after the initial inquiry “that might undermine the initial reasonable conclusion of third-party apparent authority are generally immaterial.”

It might be argued that objectively there was no ambiguity to the question of ownership, since based on what was known to officers at the time, it appeared Michelle did, in fact, have common authority over the computer. Still, the minimal step of simply checking to see if the computer was password protected would clearly have created such ambiguity. In a sense, the court of appeals recognized this when it stated in a footnote of the opinion, “[w]e do not hold that the officers could rely upon apparent authority to search while simultaneously using mirroring or other technology to intentionally avoid discovery of password or encryption protection put in place by the user.” With this statement, the court is exactly right. The problem, however, is that by not performing an initial check for password protection, law enforcement is purposefully avoiding the question altogether; the majority has implicitly held what it explicitly stated not to hold. More importantly, the burden of doing such a spot check is absurdly minimal. It would take literally seconds to complete, and the answer to the examination is, in reality, critical to the constitutionality of the search, as it constitutes the key determinant of whether the belief of apparent authority is objectively reasonable.

In the Tenth Circuit, United States v. Andrus acts as another example of courts seemingly skirting the issue of password protection. Andrus involved the investigation of a website providing users access to child pornography, which led to the suspicion that a computer in the Andrus household also contained images of this nature. Federal agents did not find the defendant at home, but instead found the defendant’s 91-year-old father, Dr. Bailey Andrus. The defendant Ray Andrus’s computer was

69 Id. at 555.
70 Id.
71 United States v. Morgan, 435 F.3d 660, 664 (6th Cir. 2006).
72 Buckner, 473 F.3d at 556 n.3 (emphasis added).
73 United States v. Andrus, 483 F.3d 713 (10th Cir. 2007).
74 Id. at 713.
75 Id.
in Ray’s bedroom with the door open, so the agents proceeded to ask a few questions before they received consent from Dr. Andrus “to search the house and any computers in it.” The agents questioned whether Ray paid rent and whether Dr. Andrus had free access to his son’s bedroom. Dr. Andrus indicated that his son did not pay rent, but that if the door were closed to his son’s room he would always knock before entering. However, the officers did not ask the much more obvious question of whether Dr. Andrus owned the computer or even used it if he was in fact the owner.

From there, Bureau of Immigration and Customs Enforcement Special Agent Kanatzar proceeded to use a combination of computer hardware and software known as EnCase to copy the entire contents of Ray’s hard drive without ever turning on the computer. EnCase “allowed him direct access to the hard drive without first determining whether a user name or password were needed.” Only later, upon examining the contents of the hard drive, did Kanatzar realize that Ray’s files were password protected. At some point after the search had commenced, a further inquiry was posed to Dr. Andrus regarding his apparent authority to consent to the search. Dr. Andrus indicated that the computer in his son’s room was the only one in the house and that the Internet service was part of the cable package. About this time, Ray Andrus himself became aware of the search because his father called him at work. The special agents then decided to discontinue the search.

After indictment, Andrus attempted to have the evidence suppressed, arguing his father’s consent lacked both actual and apparent authority. The district court agreed that Dr. Andrus lacked actual authority, considering he “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.” Yet after acknowledging that the issue of apparent authority was a “close call,” the court concluded that the agents’ belief in Dr. Andrus’s authority “was reasonable up until the time they learned there

76 Id.
77 Id.
78 Id. at 713–14.
79 Id. For more information about EnCase, see Greg Johnson, Dealing with E-Data: Using EnCase in E-Discovery, Part II, Lawyer’s PC (Thomson/West, Rochester, N.Y.), Apr. 1, 2004. Note that EnCase can also recover data that the user had previously “deleted” from his hard drive, id., and that “EnCase has been successfully admitted into evidence in thousands of criminal and civil court cases.” Id.
80 Andrus, 483 F.3d at 714.
81 Id.
82 Id.
83 Id.
84 Id. at 715.
85 Id.
was only one computer in the house." The district court concluded Dr. Andrus had apparent authority because of the following facts: first, the e-mail address used to register with the service providing child pornography was bandrus@kc.rr.com, an address associated with Dr. Bailey Andrus; second, Dr. Andrus told the investigating agents he paid for the Internet service; third, the agents were aware that more than one individual lived in the household; fourth, Ray Andrus's bedroom was not locked, so it was safe to assume other household members could enter the room freely; and fifth, Ray's computer was in plain view upon entry into the bedroom.

At the appellate level, the Tenth Circuit upheld the search, but again noted the duty for an officer presented with ambiguous facts to investigate further before relying on potentially illegitimate consent. Furthermore, it conceded the ever-growing amount of value individuals place on the privacy of their home computers, stating that, "[f]or most people, their computers are their most private spaces." This sentiment is especially evident in the modern computer era through the increased usage of thumbprint readers for laptops and the growing number of individuals who keep data stored in digital rather than paper formats (examples include taxes, business documents, spreadsheets, etc.). The biggest concession the Andrus majority made, however, was the recognition that, unlike traditional locked boxes where the lock is readily visible from the outside, determining when a computer is "locked" via password protection is impossible without first starting up the computer and attempting to access particular files. In the court's own words, "[a] critical issue in assessing a third party's apparent authority to consent to the search of a home computer... is whether law enforcement knows or should reasonably suspect because of surrounding circumstances that the computer is password protected."

Despite these issues, the majority believed that the situation was not ambiguous enough to begin with for the special agents to have to ask any further questions about Dr. Andrus's authority. The court was not persuaded by arguments that the burden on officers to make a more detailed query in the situation was extremely minimal. The problem with the majority's approach, however, is that it creates the same incentive found in Buckner, i.e., the incentive not to investigate uncertainty. This rationale will find difficulty aligning with previous Fourth Amendment jurisprudence.

86 Id.
87 Id.
88 Id. at 717 (quoting United States v. Kimoana, 383 F.3d 1215, 1222 (10th Cir. 2004)).
89 Id. at 718 (emphasis added) (quoting United States v. Gourde, 440 F.3d 1065, 1077 (9th Cir. 2006) (en banc) (Kleinfeld, J., dissenting)).
90 Id. at 718–19.
91 Id. at 719.
92 Id. at 721.
93 Id.
on the subject, considering apparent authority was never intended to be a sweeping way for law enforcement to justify searches they suspected they would not normally be able to perform; rather, dating all the way back to Stoner, the Supreme Court has consistently worked to narrow the apparent authority doctrine, not to broaden its reaches. More in-depth analysis demonstrates that Buckner and Andrus are inconsistent with the Rodriguez requirements.

C. A Better Approach—The Andrus Dissent and Trulock v. Freh

While the majority of courts have allowed apparent authority hard drive searches to be upheld despite the undiscovered password objection, some case law favors the opposite result. These courts have keenly recognized that password protection can make or break the validity of the consenter's apparent authority and the key inquiries that must be made literally take but seconds during an investigation. Based largely upon these two premises, these judges have made the wise decision to require more from law enforcement in such a context, not less.

The best example of this line of reasoning is from Judge McKay in the Andrus dissent. Here, Judge McKay recognized the tendency for law enforcement to desire to bypass the password issue altogether. He believed that the majority effectively gave a free pass to law enforcement to "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." Noting that password protection is extremely commonplace for personal computers in today's world, he also recognized the minimal burden upon law enforcement to identify ownership, stating that "[a] simple question or two would have sufficed."

Judge McKay also took note of the then newly-decided Supreme Court consent case of Georgia v. Randolph, where Chief Justice Roberts explicitly stated, "[t]o 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." Roberts' words breathe new light into the questions jurists must ask under Katz and Kyllo. When it
appears that the computer user has taken an extra step to password-protect his files, the Roberts declaration in this context certainly suggests that no third-party consent to a search of those files would be valid. But, what if under Roberts' analysis, officers turn a blind eye to whether or not the person locked his materials in the first place?

Judge McKay was reluctant in the Andrus dissent to place the burden to speak up about Dr. Andrus's lack of ownership on Dr. Andrus himself rather than the special agents.99 This is because it was not obvious to Dr. Andrus that the EnCase software was specifically designed to bypass any password protection but was clearly obvious to the special agents. Judge McKay illuminated the Fourth Amendment loophole that has been created best when he stated:

The development of computer password technology no doubt "presents a challenge distinct from that associated with other types of" locked containers . . . [However, 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, rather, it avoids it altogether, simultaneously and dangerously sidestepping the Fourth Amendment in the process.100

The McKay dissent concludes with the most pragmatic solution to the problem, namely to require that where computer searches rely purely on apparent authority consent, law enforcement must inquire or somehow check for the presence of password protection.101 Foremost, officers should simply ask whether the would-be consenter shares ownership of the computer or not. If the answer is no, then the inquiry ends there and the consenter has neither actual nor apparent authority. In the alternative, police should proceed to ask if the consenter has knowledge of a password's presence on the system. If password protection is in fact present, it will take but a few seconds to question the consenter's knowledge of the password and thus ascertain whether or not there is true common authority.

Originating in the same circuit as Buckner, Trulock v. Freh102 is a better example of the type of inquiries officers should have made in the Andrus case. In Trulock, the Fourth Circuit held that a live-in girlfriend lacked both actual and apparent authority to consent to a search of her boyfriend's computer files.103 The girlfriend told police that she and her boyfriend had separate password-protected files that were inaccessible to the other individual.104 Plaintiff Trulock was the former Director of the Office of

99 Id. at 724.
100 Id. at 723.
101 Id. at 725.
102 Trulock v. Freh, 275 F.3d 391 (4th Cir. 2001).
103 Id. at 403.
104 Id.
Intelligence of the U.S. Department of Energy (DOE) and the subject of a harassing investigation by the FBI, largely because he wrote a piece for the National Review criticizing the DOE’s handling of numerous administrative affairs. Trulock’s girlfriend, Conrad, was questioned at length about Trulock’s work at the DOE, and eventually she consented to a search of the apartment and all the computers in it (this consent was later found to be made under coercion). Despite her insistence that she and Trulock maintained completely separate log-in identities on the computer and that his files were independently password protected, two FBI Special Agents searched Trulock’s files for ninety minutes and later confiscated the hard drive without a warrant.

Weeks later, Trulock and Conrad filed a Bivens suit, which allows individuals to bring a civil suit against a federal officer for damages stemming from a constitutional violation. The plaintiffs claimed, inter alia, that the search violated their Fourth Amendment rights and that Conrad had no authority to consent to it. The Fourth Circuit Court of Appeals agreed, concluding that since Trulock used a password, he “affirmatively intended to exclude Conrad and others from his personal files.” The court also recognized that Trulock had a reasonable expectation of privacy in his files; since he concealed his password from Conrad, he could not possibly have assumed the risk that Conrad would assent to a common authority search.

Further examples where proper consideration has been given to the issue of password protection in apparent authority searches come from the Sixth Circuit Court of Appeals and the Central District of Illinois. In United States v. Aaron, the Sixth Circuit upheld a third-party consent search of the defendant’s computer following suspicion that he had violated child protection laws. In so doing, the court paid special attention to the fact that the defendant “did not protect his computer with a password or otherwise manifest an intention to restrict [the consentor’s] access.” This fact was also properly noted by the officer on duty at the time he initially began the search. Likewise, in United States v. Smith, the Central District of Illinois included in its list of factors supporting the third-party consent

105 Id. at 397–98.
106 Id. at 398–402.
107 Id. at 398.
109 Trulock, 275 F.3d at 399.
110 Id. at 403.
111 Id.
112 United States v. Aaron, 33 F. App’x 180 (6th Cir. 2002).
113 Id. at 184.
114 Id. at 182.
of a computer search the fact that "none of the officers who searched the computer found passwords," indicating that this "belies Defendant's claim of exclusive and possessory control." Both of these courts astutely saw that password protection is practically the whole ball game as to whether the third-party consenter has apparent authority and, thus, whether the search should be allowed.

D. Passwords Indicate a Subjective Expectation of Privacy

It is notable that the Trulock court did something the Buckner court and the Andrus majority did not—it weighed in its analysis the affirmative steps that the searched party took to maintain a certain level of privacy. While not specific to the computer context, the Fourth Circuit case of United States v. Pressler speaks to the issue of a defendant's expectations of privacy when he goes to great lengths to keep an item private. The Pressler court overturned a third-party consent search of the defendant's locked briefcases that a friend was looking after for safe-keeping. The court stated that, "[t]he very act of locking [the briefcases] and retaining either the key or the combination to the locks . . . was an effective expression of the defendant's expectation of privacy." It further noted that, "the defendant's failure to give [the consenter] a key or combination to the locks was the clearest evidence that there was no intention on [his] part to give . . . anyone . . . 'access' to the locked briefcases." The only difference between Pressler and Andrus is that the locks on Andrus's computer were not visible while the locks on Pressler's briefcases were. This critical examination of a subject's expectation of privacy has existed in Fourth Amendment jurisprudence since 1967, but it never even enters the picture when courts uphold hard drive searches based upon an apparent authority that is shaky at best. Rather, by dodging the issue of whether the computer has password protection on some or all of its files, one can never know just how private the searched party intended to keep his or her files in the first place.

Furthermore, the refusal to recognize that password protection is practically universalized in today's era of personal computing amounts to a failure to take judicial notice of commonly known information. The vast

116 United States v. Pressler, 610 F.2d 1206 (4th Cir. 1979).
117 Id. at 1214–15.
118 Id. at 1213–14.
119 Id. at 1214 (emphasis added).
121 See United States v. Andrus, 483 F.3d 711, 715 (10th Cir. 2007) (noting that the District Court "indicated the resolution of the apparent authority claim in favor of the government was a 'close call').
majority of personal computer users employ a Microsoft Windows–based operating system, which has the ability to separate users with unique IDs and passwords. With the addition of other common operating systems such as Mac OS X and Linux (both of which have some level of password protection available to users), almost all of today’s personal computers have at least the ability to enable password protection, and many of the operating systems either encourage or require it upon installation.

Finally, one noteworthy error that the Andrus majority made in its analysis was the recognition that computer locks are invisible and, thus, constitute new territory for law enforcement officials. In reality, however, this is a distinction without a difference. Not all locks exist in plain view in the brick and mortar world either, but this reality does not stop police officers from investigating the nature of a locking mechanism before bulldozing through it. For example, locks on briefcases and lockers can be hidden, while locks on high-security doors can be concealed in a keystroke or only seen on the other side of the door. Moreover, just because “a computer password ‘lock’ may not be immediately visible does not render it unlocked,” as computers “do exhibit [some] outward signs of password protection,” such as log-in screens and screen saver reactivation passwords. In more traditional search and seizure cases, law enforcement’s mere discovery of a lock does not end the inquiry. Rather, the state must proceed to question the consenting party about his or her knowledge of and access to the locked area before it establishes what kind of authority the consenter really has. Ultimately, there is no compelling reason why computers should be treated any differently.


124 United States v. Andrus, 483 F.3d 711, 718 (10th Cir. 2007).

125 Id.

IV. ADDITIONAL CONSIDERATIONS

A. The Location of the Computer

The location of the computer in the household gives an obvious indication as to whether or not common authority exists. A search initiated upon a computer located in a locked bedroom would not withstand scrutiny under apparent authority, whereas a computer located in an open access area of the house very well may. This distinction was taken into consideration in *Buckner*, where the court deemed it pertinent that the computer was located in a common area of the house and no one was excluded from using it.  

It also played a factor in the *Andrus* decision, as the majority relied on the fact that Dr. Andrus had open access to the defendant's bedroom to help establish valid apparent authority.

Other cases to consider computer location include *United States v. Morgan*—where the computer was located in a common area of the house and the wife maintained she occasionally used the computer—and *United States v. Smith*, where the court found apparent authority because the desk and computer were in a common area surrounded by children’s toys. Clearly, the location of the computer should be a factor taken into consideration by courts in reviewing the officers' reliance on the given apparent authority. Moreover, if the computer happens to be situated in a location similar to that in *Andrus*, state agents should proceed with caution to be sure that the consenting party truly has common authority.

B. The Scope of the Consent Given

As another facet of maintaining the validity of an apparent authority search, officers must ensure that the consent is, in fact, consenting to the search of the computer along with the rest of the house. This issue did not appear to be of concern in *Andrus*, as officers clearly asked to search both the house and any computers in it.  

However, any consent that is not broad enough or ambiguously broad when first given can certainly work to invalidate a search. In *United States v. Turner*, for example, the scope of the defendant's consent to search his apartment for evidence of an intruder who broke into a neighboring apartment was exceeded when it extended to a search of his computer files.  

Similarly, commentators analyzing the

128 United States v. Andrus, 483 F.3d 711, 721 (10th Cir. 2007).
131 *Andrus*, 483 F.3d at 713.
132 United States v. Turner, 169 F.3d 84, 86–87 (1st Cir. 1999).
Supreme Court’s decision in *Florida v. Jimeno* have stated that “[t]he scope of a consent search may not exceed the scope of the consent given. The scope of consent is determined by asking how a reasonable person would have understood the conversation between the officer and the suspect or third party when consent was given.”

Finally, it is clear that scope matters even in the context of a warrant. The Tenth Circuit case of *United States v. Carey* held that an officer exceeded the scope of a warrant authorizing a computer search for evidence of drug crimes when the officer found and continued to search for child pornography on a defendant’s computer. Applying this decision to the computer context, officers must be cautious not to take statements from a consenter allowing them to “search the entire house” or “search the apartment” without something more as permission to search a roommate’s or housemate’s entire computer. Relying on the same rationale from *Block* and *Pressler*, these searches would not withstand constitutional scrutiny.

**C. The Invasiveness of the Technology Used**

*Kyllo* makes clear that the more invasive a technology and the more likely the public is unaware of the technology’s existence, the more probable it is that a warrantless search will be overturned on Fourth Amendment grounds. Furthermore, the decision indicates that the court’s role with new privacy-invasive technology is to protect citizens where “the technology in question is not in general public use.” The ability of new technologies to invade and slowly destroy individuals’ privacy is virtually limitless, and it remains doubtful whether software like EnCase is well known to the public at large. In fact, EnCase may just be the tip of the iceberg—currently, allowing law enforcement to use software like EnCase is analogous to merely allowing them to bypass a low quality padlock on a locker. Still, with constantly improving technology (especially in the field of password protection), future software or hardware combinations will likely be even more adept at bypassing the latest encryption or even the most serious efforts to keep our computer files private. Today we allow the police to sidestep a padlock, tomorrow it is a steel–reinforced doorway.

137 Id. at 34.
CONCLUSION

In adapting the concept of apparent authority and its limitations to the area of computer searches, the added requirements for law enforcement should be simple and easy to follow. In apparent authority searches, officials need only check for password protection before initiating the search, and, if such protection exists, inquire into its nature. When taken in conjunction with the fact that 1) password protection is entirely commonplace for computers today, 2) the burden of this additional inquiry is minimal in terms of both time and effort, and 3) not making the inquiry creates the incentive for authorities to bypass the most objective and important question as to whether apparent authority exists, the response is clear: as part of establishing the validity of a third-party consent-based search of a computer under Illinois v. Rodriguez, officers should be required to follow the Andrus dissent's recommendations.

138 United States v. Andrus, 483 F.3d 711, 725 (10th Cir. 2007).