UIC John Marshall Journal of Information Technology & Privacy Law

Volume 26
Issue 1 *Journal of Computer & Information Law - Fall 2008*

Article 4

Fall 2008

United States v. Andrus: Password Protect Your Roommate, Not Your Computer, 26 J. Marshall J. Computer & Info. L. 183 (2008)

Sarah M. Knight

CASENOTE

UNITED STATES V. ANDRUS: PASSWORD PROTECT YOUR ROOMMATE, NOT YOUR COMPUTER

SARAH M. KNIGHT*

I. INTRODUCTION

"It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."[1] This statement becomes more relevant each year as new developments in technology change the way we live our lives. Recently, Chief Justice Roberts commented that cases involving emerging technologies and search and seizure are the cases that "people will look back on one day and say were significant."[2] Perhaps, *United States v. Andrus* will become such a case.[3]

In *United States v. Andrus*, a case of first impression, the Tenth Circuit, addressed the expectation of privacy associated with a home computer in third-party consent situations.[4] In *Andrus*, the court was

* J.D. Candidate, 2009, The John Marshall Law School. I would like to thank Paul Pendley for bringing the *Andrus* case to my attention. A special thanks is due to members of The John Marshall Journal of Computer & Information Law for their help in editing this article.

1. Kyllo v. United States, 533 U.S. 27, 34 (2001).

2. Tad Walch, *Tech Cases Critical, Roberts Says at Y.,* DESERET MORNING NEWS, Oct. 24, 2007, http://findarticles.com/p/articles/mi_qn4188/is_/ai_n21060074 (last visited Nov. 7, 2008). Justice Alito has also commented on the effect new technology is having on Fourth Amendment jurisprudence: "What constitutes a "search and seizure" online is a critical law debate and is constantly reshaping the Fourth Amendment. . .Now we're entering this new virtual world . . . and we have to translate the precedents and principles we have dealing with physical grounds to the world of electronic communication." Eric Roper, *Supreme Court Justice Alito Presides in Moot Court Event*, THE GW HATCHET, Feb. 7, 2004, *available at* http://media.www.gwhatchet.com/media/storage/paper332/news/2007/02/05/News/Supreme.Court.Justice.Alito.Presides.In.Moot.Court.Event-2695147.shtml.

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

4. *Id.*

presented with the "narrow question of the apparent authority of a homeowner to consent to a search of a computer on his premises" where the homeowner had computer access, an Internet account, and an e-mail address used to register on a child pornography website.[5] The court held the search of Andrus' computer was valid based on his father's consent to the search.[6] Under the totality-of-the-circumstances test,[7] the facts known to the officers at the time the computer search commenced created an "objectively reasonable perception" that the father had apparent authority to consent to the search of the computer.[8] The court further stated that even if Andrus' father could not actually use the computer and it was password protected, "these mistakes of fact do not negate his apparent authority"[9] because officers did not need to determine if a password was in place to assess the father's apparent authority.[10]

The dissent found the use of forensic software presented a problem in third-party consent cases.[11] It suggested that in warrantless searches based on consent, law enforcement should be required to "check for the presence of password protection and, if a password is present, inquire about the consenter's knowledge of that password and joint access to the computer."[12]

The Tenth Circuit erred by not requiring law enforcement officials to check for password protection before commencing a computer search. The court's decision is contrary to the rationale behind the third-party consent exception to the Fourth Amendment[13] warrant requirement.[14] As a consequence of this holding, third-parties can consent to searches beyond their authority, and individuals' efforts to secure their data are rendered useless.

---

5. United States v. Andrus, 499 F.3d 1162 (10th Cir. 2007).

6. *Andrus*, 483 F.3d at 722.

7. The totality-of-the-circumstances test is an objective inquiry into whether, at the time the search begins, the facts available to the officers "would lead a reasonable officer to believe the third party had authority to consent to the search." *Id.* at 716-17.

8. *Id.* at 722.

9. *Id.*

10. *Id.* at 720 n.6.

11. *Id.* at 723 (McKay, J., dissenting).

12. *Id.* at 725.

13. "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV.

14. *See* Illinois v. Rodriguez, 497 U.S. 177 (1990) (extending third-party consent doctrine to situations where apparent authority exists); United States v. Matlock, 415 U.S. 164 (1974) (establishing actual authority doctrine of third-party consent based on assumption of risk). For a discussion of the development of actual authority and apparent authority, *see infra* text accompanying notes 115-22.

This Casenote asserts that the Tenth Circuit's avoidance of the issues surrounding the use of EnCase in third-party consent searches will create confusion for law enforcement and courts in future cases. The approach posited by the dissent in *Andrus*,[15] in conjunction with other circuits' treatment of similar issues,[16] better resolves the controversy that will likely surround the use of EnCase in future searches. This rule also remains consistent with the principles of the third-party consent exception. In warrantless searches based on third-party consent, law enforcement should be required to check for password protection on computers before commencing a search. If password protection is present, officers must ask the consenter whether he or she knows the password.[17] If the consenter does not know the password, the use of software such as EnCase to bypass the password protection should be prohibited without a warrant.

This Casenote contends the dissent in *Andrus* is correct and the rule set forth in the dissenting opinion should be followed. Beginning with a brief summary of the facts, background, and issue presented, the necessary foundation for understanding the analysis of the decision is outlined. This Casenote will also address the court's analysis by examining both the majority and dissenting opinions. Finally, a detailed critique and proposal for alternative disposition is presented.

II. SUMMARY OF FACTS AND BACKGROUND

At approximately 8:45 a.m. on August 27, 2004, an agent of the Bureau of Immigration and Customs Enforcement ("ICE") and a Leawood Police detective knocked on the door of the Andrus' residence for a "knock and talk" interview, hoping to conduct a consent search.[18] The

15. *Andrus*, 483 F.3d at 725 (McKay, J., dissenting).

16. *See* United States v. Buckner, 473 F.3d 551, 556 (4th Cir. 2007) (finding apparent authority of third party consent valid where no password protection was in place); Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir. 2001) (concluding the third party did not have authority to consent to the search where she had access to the hard drive but not the defendant's password-protected files). *Infra* pt. V.A. (discussing both cases with regard to the importance of password protection in assessing third-party consent).

17. *Andrus*, 483 F.3d at 725 (McKay, J., dissenting).

18. Agents believed they did not have enough information to obtain a search warrant for the residence so they were using the "knock and talk" interview to gather more information. *Id.* at 713. A "knock and talk" interview occurs where an officer approaches a residence, identifies himself to the occupant, and asks to come in to talk. United States v. Gomez-Moreno, 479 F.3d 350, 355 (5th Cir. 2007). The goal of the interview is to gain information or, if the officer reasonably suspects criminal activity, to obtain consent for a search. *Id.* However, an officer does not need to have reasonable suspicion before conducting a "knock and talk" interview. United States v. De Jesus Cruz-Mendez, 467 F.3d 1260 (10th Cir. 2006) (citing cases and characterizing the "knock and talk" as a "consensual encounter" which does not violate the Fourth Amendment).

agents were interested in Ray Andrus ("Ray") in connection with their investigation of a company that provided subscribers with access to websites containing child pornography.[19]

Dr. Bailey Andrus, age ninety-one, answered the door in his pajamas and invited the agents in.[20] The agents soon learned from Dr. Andrus that his son, Ray, lived in the center bedroom of the residence, but he was not at home.[21] ICE Special Agent Cheatham noticed the door to Ray's bedroom was open and asked Dr. Andrus whether he had access to the bedroom. Dr. Andrus told the officers "he felt free to enter the room when the door was open, but always knocked if the door was closed."[22]

Special Agent Cheatham asked Dr. Andrus for permission to search the house and any computers in it.[23] Dr. Andrus signed a written consent form and led Cheatham to Ray's bedroom to show him where the computer was located.[24] Agent Cheatham then went outside to bring ICE Special Agent Kanatzar, a forensic computer expert, into the residence.[25] Kanatzar entered Ray's bedroom and began assembling his forensic equipment.[26] Ray's computer was turned off at the time Kanatzar entered the room.[27] Kanatzar attached his own laptop and government equipment to Ray's computer in about the first ten to fifteen minutes after entering the room.[28] Then, without turning the computer on,[29] Kanatzar used EnCase[30] forensic software to examine the contents of the computer's hard drive.[31]

EnCase is a line of software products used in computer forensics sold

---

19. "Ray Andrus" was a subscriber with the company and listed his address on West 81st Terrace, an address the driver's license bureau and post office showed to be used by Ray Andrus, Bailey Andrus, and Richard Andrus. *Andrus*, 483 F.3d at 713. The credit card number on the account belonged to Ray, and the e-mail address provided to the company was "bandrus@kc.rr.com," which was determined to be associated with Dr. Bailey Andrus. *Id.* The investigation into the Andrus residence began in January 2004 and focused primarily on Ray. *Id.*

20. *Id.*

21. *Id.*

22. *Id.*

23. *Id.*

24. *Andrus*, 483 F.3d at 713.

25. *Id.*

26. *Id.*

27. *Id.* at 723.

28. *Id.* at 713.

29. *Id*.

30. EnCase is a registered trademark of Guidance Software, Inc. *See* Guidance Software, http://www.guidancesoftware.com/products/ef_index.aspx (last visited Sept. 23, 2007) (EnCase Forensic product page).

31. Other software programs are available to access hard drives and create forensic copies. *See*, *e.g.,* SafeBack by New Technologies, Inc., http://www.forensics-intl.com/safeback.html (last visited Sept. 23, 2007); Ultimate Toolkit and Forensic Toolkit, http://www.accessdata.com/common/pagedetail.aspx?PageCode=prodfor (last visited Sept. 23, 2007);

by Guidance Software, Inc.[32] EnCase can be used to create copies of computer hard drives or removable media, such as flash drives and CDs.[33] EnCase creates a "self-authenticated bit stream image of the data," which preserves the data in its original state while it is being copied.[34] This bit stream image or copy, also known as a forensic copy, is a mirror image of the original drive.[35] The copy created by EnCase includes all types of hidden information,[36] including files in unallocated

---

RALPH D. CLIFFORD, CYBERCRIME: THE INVESTIGATION, PROSECUTION, AND DEFENSE OF A COMPUTER-RELATED CRIME 161 n.173 (2001).

32. Guidance Software, EnCase Forensic, http://www.guidancesoftware.com/products/ef_index.aspx (last visited Sept. 23, 2007). There are over 20,000 licensed users of EnCase technology, including both government and private entities. Press Release, Guidance Software, Guidance Software to Announce Third Quarter 2007 Financial Results on Tuesday, November 13, 2007 (Oct. 9, 2007), *available at* http://investors.guidancesoftware.com/releasedetail.cfm?ReleaseID=267917 (last visited Mar. 4, 2009). The Federal Bureau of Investigation, the U.S. Department of Homeland Security, the U.S. Department of Defense, and the New Scotland Yard use EnCase software. Guidance Software, EnCase Forensic LE 1, http://www.guidancesoftware.com/downloads/getpdf.aspx?fl=.pdf (last visited Sept. 23, 2007) (company product brochure).

33. Guidance Software, http://www.guidancesoftware.com/products/ef_works.aspx (last visited Sept. 23, 2007) (EnCase Forensic product page).

34. Guidance Software, EnCase Field Intelligence Model 3, http://www.guidancesoftware.com/downloads/getpdf.aspx?fl=.pdf (last visited Sept. 23, 2007) (company product brochure).

35. State v. Cook, 777 N.E.2d 882, 886 (Ohio Ct. App. 2002). The court discussed the acquisition and search of the defendant's hard drive in reviewing an objection to the reliability of the process to make mirror image copies. *Id.* Because EnCase enables officers to create a mirror image copy of the hard drive to analyze later, the use of EnCase in criminal investigations necessarily implicates a discussion of the reasonableness of the data seizures. *Id.* However, the scope of this Casenote is limited to a discussion of officers' use of EnCase to search data on electronic drives. For an analysis of whether using forensic software to copy a hard drive is a search or a seizure, see Susan W. Brenner & Barbara A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 MICH. TELECOMM. & TECH. L. REV. 39, 107 (concluding that, for policy reasons, copying data should be considered a seizure under the Fourth Amendment).

36. Files can be "hidden" so they do not appear in directory listings. Another simple yet effective way to hide files and data is to give them a generic file name or extension that would not necessarily raise any flags in a search. For example, a person could name a file he wants to be hidden, such as a child pornography image, "format.exe." Craig Ball, *Computer Forensics for Lawyers Who Can't Set a Digital Clock* 32-3, http://www.craigball.com/CF_0807-Digital%20Clock%20article%20only.pdf (2007) (last visited Sept. 23, 2007). This is where software such as LTU Technologies' Image-Seeker hopes to render these efforts useless by using "image DNA" to recover these files, regardless of the name or file extension. *Infra*, note 50.

space,[37] hidden processes,[38] and, in most cases, previously deleted files.[39]

EnCase also has a preview function which allows examiners to view the data while it is being copied.[40] "Once image files are created, examiners can search[41] and analyze multiple drives or other media simultaneously, using keyword searches, hash analysis, file signature analysis, file-specific filters and multiple filters."[42] After EnCase analyzes the content of the drive, a report is generated detailing the findings.[43] In addition, EnCase can be used to access a hard drive without turning the computer on or determining whether a user name or password was necessary to log on to the computer.[44] Courts thus far have upheld the admissibility of EnCase's mirror image hard drives and reports.[45]

At the Andrus residence on August 27, 2004, Special Agent Kanatzar used EnCase's preview utility[46] to examine the contents of Ray's hard drive.[47] EnCase allowed Kanatzar direct access to the hard drive without first determining whether the system had a user name or password.[48] In this case, Ray's computer did have a user profile, and without EnCase, the agents would have needed his name and password to access files stored under that profile.[49] Kanatzar used EnCase to

37. Unallocated space is an area marked available for data storage but not yet overwritten by other data. Thus, the deleted data is still present in the space. Ball, *supra* note 36, at 8, 25.

38. Guidance Software, EnCase Field Intelligence Model, *supra* note 33, at 3.

39. JOHN PATZAKIS & VICTOR LIMONGELLI, GUIDANCE SOFTWARE, ENCASE LEGAL JOURNAL 25 (Apr. 2007), *available at* http://www.guidancesoftware.com/downloads/getpdf.aspx?fl=.pdf.

40. Guidance Software, EnCase Forensic LE, *supra* note 32. This function is similar to listening to a song while it is being downloaded, or watching a television show being recorded on a digital video recorder while it is being recorded.

41. Each computer search begins with the creation of the mirror image copy, which is saved as a "read only" file so it cannot be altered. Analysts search only this file, so the actual search occurs on the government's computer, not the suspect's. Orin Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 540 (2005).

42. Guidance Software, EnCase Forensic LE, *supra* note 32.

43. Guidance Software, http://www.guidancesoftware.com/products/ef_works.aspx (last visited Sept. 23, 2007) (EnCase Forensic product page).

44. U.S. v. Andrus, 483 F.3d 711, 713-14 (10th Cir. 2007).

45. *See* State v. Cook, 777 N.E.2d 882, 887 (Ohio Ct. App. 2002) (stating there was "no doubt that the mirror image was an authentic copy of what was present on the computer's hard drive"); Taylor v. State, 93 S.W.3d 487, 507 (Tex. App. 2002) (holding the computer-generated report from EnCase was not hearsay).

46. Guidance Software, EnCase Forensic LE, *see supra* text accompanying note 40.

47. JOHN PATZAKIS & VICTOR LIMONGELLI, GUIDANCE SOFTWARE, ENCASE LEGAL JOURNAL 25 (Apr. 2007), *available at* http://www.guidancesoftware.com/downloads/getpdf.aspx?fl=.pdf.

48. *Andrus*, 483 F.3d at 713-14.

49. *Id.*

search for .jpg picture files[50] and traced the images he retrieved to particular folders on the hard drive.[51] Once the search process began, it took approximately five minutes to view images of child pornography.[52] Ray was arrested and indicted on charges of knowingly and intentionally possessing pornographic images of minors.[53]

At his trial in the United States District Court for the District of Kansas, Ray moved to suppress the evidence gathered from the search of his residence and computer based on his father's consent.[54] He argued that: (1) Dr. Andrus' consent was not voluntary; (2) Dr. Andrus lacked actual authority to consent to a search of Ray's bedroom; and (3) Dr. Andrus lacked apparent authority because he "could not reasonably be seen as having authority to consent to a search of the computer."[55] At an evidentiary hearing, the district court found that Dr. Andrus' consent was voluntary, but he lacked actual authority to consent to the computer search.[56] However, the district court concluded that Dr. Andrus had apparent authority to consent to the search.[57] Accordingly, the district court denied the motion.[58]

On appeal to the Tenth Circuit, Ray contested the district court's

---

50. Files with a ".jpg" extension attached to the file name usually contain a photograph or graphical image. *Andrus*, 483 F.3d at 714 n.2 (citing United States v. Walser, 275 F.3d 981, 984 n.3 (10th Cir. 2001)). Another company, LTU Technologies, has developed software to work alongside EnCase in searching for images. LTU Technologies, Image-Seeker for EnCase 1-2, http://www.ltutech.com/en/PDFs_Eng/Image-Seeker_for_Encase.pdf (last visited Nov. 4, 2007). Image-Seeker for EnCase (ISE) "uses digital signatures ("image DNA") to index, recognize and describe images according to their visual content." *Id.* Image-Seeker detects camouflaged files (hidden images with fake file extensions) and images modified by criminals (*e.g.* an image with a black box placed over a child's face). *Id.* Image-Seeker is applicable to fraud, counterfeiting, abusive images, counter-intelligence, and counter-terrorism investigations. *Id.* Image-Seeker is used by the Federal Bureau of Investigation and the U.S. Department of Homeland Security (Immigration and Customs Enforcement – Cyber Crimes Center). *Id.*

51. *Andrus*, 483 F.3d at 714.

52. Special Agent Cheatham interrupted Kanatzar's search after Cheatham had continued his conversation with Dr. Andrus. *Id.* Cheatham learned that Ray's computer was the only computer in the house and that the Internet service was part of the cable package. *Id.* At that point, Dr. Andrus called Ray at work and spoke with him briefly before handing the phone to Cheatham. *Id.* Ray agreed to meet the agents back at the house and arrived ten to twenty minutes later. *Id.* Cheatham told Andrus that a computer technician was there and Dr. Andrus had consented to a search of the house and the computer. *Id.* Cheatham then obtained Ray's verbal consent and instructed Kanatzar to continue the search. *Andrus*, 483 F.3d at 714.

53. 18 U.S.C. § 2252(a)(4)(B) (2000).

54. *Andrus*, 483 F.3d at 715.

55. *Id*.

56. *Id*.

57. *Id*.

58. *Id*. at 716.

ruling on Dr. Andrus' apparent authority.[59] He argued the officers faced an ambiguous situation at the time of the search.[60] This situation required them to further inquire about Dr. Andrus' authority to consent prior to beginning the search.[61] Rejecting Ray's argument, the Tenth Circuit concluded Dr. Andrus had apparent authority to consent to the computer search and affirmed the denial of the motion to suppress.[62] The court also noted, "determining whether a password was actually in place. . .is unnecessary for analyzing Dr. Andrus' apparent authority, since the password would not have been obvious to the officers at the time they obtained consent and commenced the search."[63] Not all of the judges agreed with this line of reasoning, though.

The dissent found the use of EnCase presented a problem in third-party consent cases and suggested that in "consent-based, warrantless computer searches," law enforcement should be required to "check for the presence of password protection and, if a password is present, inquire about the consenter's knowledge of that password and joint access to the computer."[64] The dissent also stated that, given the ambiguities in this case, "the circumstantial evidence is simply not enough to justify the agents' use of EnCase software without making further inquiry."[65]

Ray Andrus filed a petition with the Tenth Circuit for an en banc hearing.[66] The panel denied rehearing, but noted the opinion was limited to the narrow fact situation presented in the case.[67] The panel further stated that the questions not presented and for which there is no factual development are: (1) "the extent and capability and activation of password protection or user profiles on home computers"; (2) "the capability of EnCase software to detect the presence of password protection or a user profile"; and (3) the degree to which law enforcement confronts password protection or user profiles on home computers.[68]

---

59. *Id*.

60. *Andrus*, 483 F.3d at 716.

61. Ray also argued that "his own consent, given after the allegedly illegal computer search yielded inculpatory evidence, did not cure the alleged illegality because the earlier search and his later consent were not sufficiently attenuated." *Id*. Since the court determines that Dr. Andrus had apparent authority to consent to the search, it does not address the validity of Ray's subsequent consent. *Id*. at 722.

62. *Id*. at 716.

63. *Id*. at 720 n.6.

64. *Id*. at 725 (McKay, J., dissenting).

65. *Id*.

66. *Andrus*, 499 F.3d at 1162.

67. *Id.*

68. *Id*. at 1162-63.

III. ISSUE PRESENTED

The issue presented to the court was whether the officers, under the totality of the circumstances known to them, could reasonably have believed Dr. Andrus had authority to consent to a search of his son's computer.[69] Focusing on the majority opinion and the dissent, the following section discusses the court's decision in detail.

IV. COURT'S ANALYSIS

A. Majority opinion

The court began its analysis by examining consent searches under the Fourth Amendment. The court referenced the fact that "voluntary consent to a police search given by . . . a third party with authority over the subject property, is a well-established exception to the warrant requirement" of the Fourth Amendment.[70] Actual authority of a third party is determined by whether he or she has either "mutual use of the property by virtue of joint access or control for most purposes."[71] A third party has apparent authority where "an officer reasonably, even if erroneously, believes the third party possesses authority to consent."[72] Since Dr. Andrus did not have actual authority, the court looked to apparent authority. To determine whether apparent authority exists, the court makes "an objective, totality-of-the-circumstances inquiry into whether the facts available to the officers at the time they commenced the search would lead a reasonable officer to believe the third party had authority to consent to the search."[73]

Assessing a third party's consent to the search of a home computer involves a determination of whether law enforcement knows or should reasonably suspect because of surrounding circumstances that the computer is password-protected.[74] Furthermore, the court noted that another factor to be considered in assessing whether apparent authority exists is where the computer is located within the home.[75] Where a computer is located in a common area accessible to others in the house, the

69. *Andrus*, 483 F.3d at 720. Because this issue is dispositive, the court did not address the validity of Ray's subsequent consent. *Supra* note 61.

70. *Id*. at 716 (citing United States v. Rith, 164 F.3d 1323, 1328 (10th Cir. 1999)).

71. *Id*. (citing *Rith*, 164 F.3d at 1329).

72. *Id*. (citing Georgia v. Randolph, 547 U.S. 103, 126 (2006)).

73. *Andrus*, 483 F.3d at 717-18.

74. *Id.* at 719. *See Trulock*, 275 F.3d at 391; United States v. Morgan, 435 F.3d 660, 663 (6th Cir. 2006) (concluding wife had apparent authority because she initiated contact with the police, computer was located in common area of the house, and wife told police that she had used computer, she and husband did not have usernames or passwords, and she had installed software on the computer).

75. *Andrus*, 483 F.3d at 719.

third party consent to search has generally been upheld.[76]

Ray Andrus contends the ambiguities in the situation facing the officers "required the officers to ask further questions concerning Dr. Andrus' authority to consent to a computer search prior to commencing the search."[77] For example, the computer was located in Ray's bedroom, rather than in a common area.[78] Also, the officers did not ask Dr. Andrus specific questions about his computer use.[79]

The court discussed the expectation of privacy in computers by comparing computers to other types of containers.[80] The court noted other cases comparing computers to "a suitcase or briefcase,"[81] and password-protected files to a "locked footlocker inside the bedroom."[82] Recognizing that users commonly store intimate information on their computers,[83] the court found that computers should fall in the same category as other personal items that "command a high degree of privacy."[84] In contrast, locks on computers are not "apparent from visual inspection of the outside of the computer, especially when the computer is turned off," like a lock on a suitcase or footlocker.[85] The court also recognized that the difficulty in determining whether a computer is locked is exacerbated by EnCase because the software can bypass user profiles and password protection.[86]

Using the totality-of-the-circumstances test, the court concluded the facts available to the officers when they commenced the search reasonably indicated that Dr. Andrus had authority to consent to the search of the computer.[87] Dr. Andrus had unlimited access to Ray's bedroom,

---

76. *Id. See* United States v. Buckner, 473 F.3d 551, 555-56 (4th Cir. 2007) (determining wife's consent was valid where wife leased computer in her name, computer was found in living room, computer was on when police arrived, and there was no indication that any of the files were password-protected); *Morgan*, 435 F.3d at 663-64.

77. *Andrus*, 483 F.3d at 716.

78. *Id.* at 720.

79. *Id.*

80. *Id.* at 718.

81. *Id.* (citing United States v. Aaron, 33 Fed. Appx. 180, 184 (6th Cir. 2006) (unpublished)).

82. *Id.* (citing *Trulock*, 275 F.3d at 403).

83. "[C]omputers are playing an ever greater role in daily life and are recording a growing proportion of it. . .[T]hey are postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more. . .Each new software application means another aspect of our lives monitored and recorded by our computers." *Andrus*, 483 F.3d at 718 (citing Orin Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 568 (2005)).

84. *Id.* (citing United States v. Salinas-Cano, 959 F.2d 861, 864 (10th Cir. 1992)).

85. *Id.*

86. *Id.* at 719 n.5.

87. *Id*. at 720.

where the computer was located.[88] Dr. Andrus paid the Internet and cable bill.[89] Also, an e-mail address with Dr. Andrus' first initial had been activated and used to register on a website providing access to child pornography.[90] The officers did not ask Dr. Andrus specific questions about his use of the computer,[91] and Dr. Andrus remained silent about any lack of authority he had over the computer.[92]

Andrus argues that password protection of home computers is so common that "a reasonable officer ought to know password protection is likely."[93] Andrus did not proffer any evidence to support this contention and, without this factual basis, the court could not take judicial notice[94] of the fact that password protection was so pervasive as to be common knowledge to an officer.[95] However, the court stated that law enforcement's use of EnCase may be questionable, if the factual basis were provided.[96] The court also noted it was unnecessary for the apparent authority analysis to determine whether a password was actually in place on Andrus' computer because the password would not have been obvious to the officers when they obtained consent and commenced the search.[97] Based on these facts, the court found the officers' belief that Dr. Andrus had apparent authority to consent to the search of the computer was reasonable.[98]

---

88. *Id*.

89. *Andrus*, 483 F.3d at 720.

90. *Id*.

91. *Id*.

92. *Id.* at 721. In assessing a parent's authority to consent to a search of an adult child's private areas in the home, courts have considered the following factors: "the suspect's age; whether the suspect pays rent; and whether the suspect has taken affirmative steps to deny his or her parents access to the suspect's room or private area. When suspects are older, pay rent, and/or deny access to parents, courts have generally held that parents may not consent." COMPUTER CRIME AND INTELLECTUAL PROP. SECTION, U.S. DEPT. OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS (2002), *available at* http://www.cybercrime.gov/s&smanual2002.htm.

93. *Andrus*, 483 F.3d at 721.

94. "A judicially noticed fact must be one not subject to reasonable dispute in that it is either (1) generally known within the territorial jurisdiction of the trial court or (2) capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned." FED. R. EVID. 201(b). Judicial notice of a fact may be discretionary or mandatory. FED. R. EVID. 201(b) and (c).

95. *Andrus*, 483 F.3d at 721.

96. *Id.* at 722 n.8.

97. *Id.* at 720 n.6.

98. *Id.* at 722.

B. DISSENT

The dissenting judge, Judge McKay, took issue with the majority's analysis of law enforcement's duty to inquire into a third party's knowledge of password protection on the computer.[99] Although the dissenting judge agreed that the majority correctly analogized computers to containers, the dissent disagreed with the characterization of the problems posed by EnCase and other software. The dissent stated that, rather than "exacerbating" the difficulty with seeing a lock on a computer,[100] by skipping past whether passwords exist, EnCase avoids the problem altogether and "sidesteps" the Fourth Amendment.[101] The dissent points out that, while the majority correctly states that a computer password is not "apparent from visual inspection of the outside of the computer, especially when the computer is turned off,"[102] computers exhibit signs of password protection once turned on.[103]

In this case, the dissent concluded the circumstantial evidence was not sufficient to justify the officers' use of EnCase without further inquiry regarding Dr. Andrus' use of the computer.[104] The dissent noted that the burden on law enforcement to identify the owner of the computer was minimal and that another question or two would likely have resolved the issue.[105] In sum, the dissenting judge concluded:

> [G]iven the case law indicating the importance of computer password protection, the common knowledge about the prevalence of password usage, and the design of EnCase or similar password bypass mechanisms, the Fourth Amendment and the reasonable inquiry rule . . . mandate that in consent-based, warrantless computer searches, law enforcement personnel inquire or otherwise check for the presence of password protection and, if a password is present, inquire about the consenter's knowledge of that password and joint access to the computer.[106]

---

99. *Id.* (McKay, J., dissenting).

100. *Id.* at 719 n.5.

101. *Andrus*, 483 F.3d at 723 (McKay, J., dissenting).

102. *Id.* at 718.

103. *Id.* at 723 (McKay, J., dissenting). As described in pt. V.C., officers cannot simply turn the computer on to check for a password. Turning the computer on will destroy evidence and compromise the integrity of the data acquired during the search. *See* Brenner & Frederiksen *supra* note 35, at 66 (describing how inadvertent spoliation can occur when searching computers for evidence).

104. *Andrus*, 483 F.3d at 725 (McKay, J., dissenting).

105. *Id.* at 724. The dissent went as far as to suggest that the officers believed that they lacked sufficient justification for a search warrant. *Id.* at 725.

106. *Id.* (internal citations omitted).

C. Appeal

Ray Andrus filed a petition for an en banc rehearing.[107] A majority of the panel voted to deny the request.[108] In denying the rehearing, the panel majority clarified the holding in *Andrus*.[109] The majority stated

> [The] opinion is limited to the narrow question of the apparent authority of a homeowner to consent to a search of a computer on premises in the specific factual setting presented, including the undisputed fact that the owner had access to the computer, paid for [I]nternet access, and had an e-mail address used to register on a website providing access to the files of interest to law enforcement.[110]

The majority also noted that "the extent of capability and activation of password protection or user profiles on home computers, the capability of EnCase software to detect the[ir] presence. . ., or the degree to which law enforcement confronts password protection or user profiles on home computers" were not questions presented in the case.[111] Ray Andrus also petitioned the United States Supreme Court for certiorari, but was denied.[112]

V. AUTHOR'S ANALYSIS

The Tenth Circuit erred in finding that the officers were not required to ask about for password protection before commencing a computer search based on third-party consent.[113] Specifically, the court's decision in *Andrus* is not in agreement with the rationale behind the third-party consent exception to the warrant requirement of the Fourth Amendment. As a result, *Andrus* is likely to result in confusion among law enforcement agencies and courts. The proper disposition of *Andrus* is the analysis and rule set forth in the dissenting opinion.

A. Third-party consent rationale

The court's decision in *Andrus* runs contrary to established principles of the third-party consent exception to the warrant requirement. The Fourth Amendment prohibits warrantless searches of an individual's home or possessions.[114] Over time, a number of exceptions have

107. *Andrus*, 499 F.3d at 1162.

108. *Id.* A majority of nine judges voted to deny rehearing. The dissenting judge from the first appeal, as well as three other judges, voted to grant rehearing. *Id.*

109. *Id.*

110. *Id.*

111. *Id.* at 1162-63.

112. Andrus v. United States, 128 S. Ct. 1738 (2008).

113. *Andrus*, 483 F.3d at 720 n.6.

114. *Id.* at 716.

evolved that dispense with the warrant requirement.[115] The watershed case for the third-party consent exception is *United States v. Matlock*.[116] In *Matlock*, the court established that consent by a third party "who possesses common authority over premises or effects is valid as against the absent, nonconsenting person with whom that authority is shared."[117] The common authority justifying the search was not premised on property law and does not derive from the mere property interest a third party has.[118] Rather, the validity of the consent rests on the "mutual use of the property by persons generally having joint access or control for most purposes."[119] The reasoning behind the exception is that one who permits joint access and control by others assumes the risk that the other persons might permit the common area to be searched.[120] Thus, the doctrine of apparent authority arose.

The third-party consent exception has been expanded to situations where an individual has apparent authority to consent to the search.[121] Apparent authority is determined by a "totality-of-the-circumstances inquiry into whether the facts available to the officers at the time they commenced the search would lead a reasonable officer to believe the third party had authority to consent to the search."[122] However, the search of an object typically associated with a high degree of privacy, such as a suitcase, might be unreasonable if it is authorized by a third party and the "officers know or should know the owner has indicated the

115. *See, e.g.*, Ohio v. Robinette, 519 U.S. 33 (1996) (establishing an exception where there is voluntary consent by the party); Illinois v. Rodriguez, 497 U.S. 177 (1990) (creating the third-party consent exception); South Dakota v. Opperman, 428 U.S. 364 (1976) (allowing a warrantless search of a car legally impounded); United States v. Matlock, 415 U.S. 164 (1974); Schneckloth v. Bustamonte, 412 U.S. 218 (1973); Vale v. Louisiana, 399 U.S. 30 (1970) (permitting a more extensive search incident to arrest when officers know evidence is "in the process of destruction" or is "about to be removed" from the jurisdiction); Chimel v. California, 395 U.S. 752 (1969) (establishing an exception for search incident to arrest); Warden v. Hayden, 387 U.S. 294 (1967) (creating an exception for exigent circumstances, specifically in hot pursuits); Carroll v. United States, 267 U.S. 132 (1925) (holding the entire car may be searched if probable cause exists and exigency created by car's mobility) .

116. *Matlock*, 415 U.S. at 164.

117. *Id.* at 169. *See also* Georgia v. Randolph, 547 U.S. 103, 122-23 (2006) ("[A] physically present inhabitant's express refusal of consent to a police search is dispositive as to him, regardless of the consent of a fellow occupant.").

118. *Matlock*, 415 U.S. at 172.

119. *Id.*

120. *Id.*

121. *See* Illinois v. Rodriguez, 497 U.S. 177 (1990) (extending third-party consent doctrine to situations where apparent authority exists).

122. *Andrus*, 483 F.3d at 716-17 (citing *Rodriguez*, 497 U.S. at 188).

intent to exclude the third party from using or exerting control over the object."[123]

The court in *Andrus* correctly analogizes computers to other containers, particularly those associated with a high expectation of privacy.[124] The court notes that computers are pervasive in American homes and that "[a] personal computer is often a repository for private information the computer's owner does not intend to share with others."[125] Further, the court compares computers to bedrooms, a person's most private space.[126] In contrast, the analysis the court employs to determine the reasonableness of the officers' belief that Dr. Andrus had authority to consent to the search does not match this comparison. The court suggests that because a lock on a computer is not readily visible from an inspection of the outside of a computer, an officer's duty to inquire about the consenting party's access is somehow lessened.[127] Requiring officers to inquire about passwords only when their presence is "obvious" is not sufficient to protect the high expectations of privacy individuals possess in the data stored on their computers.[128]

The problem is, if a third party does not know the computer's password, then he does not have joint access or control. An individual who does not give his password to another person has not assumed the risk that someone else will consent to a search. Using EnCase where officers do not know whether the consenting party has the password, or even know if one exists, diminishes the validity of the search. Whether the court requires a further inquiry or not, a search that is based on facts that are merely obvious to officers is arguably less valid than a search based on facts known to officers after a reasonable, if not minimal, inquiry. As a practical matter, gathering additional facts prior to beginning the search only enhances the government's case. While in many cases the consenting party likely will not know the password, it is better to get a search warrant and strengthen the case than have a child pornography case crumble because apparent authority cannot be established without facts the officers could have easily ascertained.

Given that computers are analogous to other objects that command a high expectation of privacy, permitting law enforcement to use EnCase as a shortcut is particularly offensive to the Fourth Amendment's protec-

123. *Id.* at 717 (citing *Salinas-Cano*, 959 F.2d at 865-66 (finding officers' belief in apartment owner's authority to consent to search of defendant's suitcase unreasonable where police failed to ask about his use of or control over the suitcase)).

124. *Id.* at 718 (citing *Aaron*, 33 Fed. Appx. at 184).

125. *Id.*

126. *Id.* (citing United States v. Gourde, 440 F.3d 1065, 1077 (9th Cir. 2006) (en banc) (Kleinfield, J., dissenting)).

127. *Id.*

128. *Andrus*, 483 F.3d at 720 n.6.

tion against unreasonable searches. The court in *Andrus* goes so far as to compare the privacy expectations for computers to that of bedrooms.[129] This comparison is ironic because the bedroom has been afforded the highest degree of protection for an individual's private affairs.[130] If courts are willing to recognize that computers and the information stored on them command a high expectation of privacy, then that level commands that the expectations for law enforcement to exercise care in preserving that right be proportionate. It could be argued that requiring officers to check for the presence of passwords and the consenter's knowledge of passwords elevates the consent to actual authority, and the doctrine of apparent authority is no longer necessary. In contrast, apparent authority is still needed where a consenter has fraudulently obtained the owner's password and officers reasonably rely on the consent. Apparent authority would also be needed where the consenter thought he knew the password, but he was wrong or the owner changed it. Special care should be taken not only when dealing with third-party consent and actual authority, but apparent authority as well.

The totality-of-the-circumstances test applied in apparent authority cases considers a number of factors, including the location of the computer within the residence.[131] While access to the room with the computer is an important consideration in assessing apparent authority, it is not as significant as access to the computer's contents itself. Also, the totality-of-the-circumstances test examines the facts known to the officers at the time they commence the search.[132] The problem with applying this test to the situation in *Andrus* is that it does not take into account whether the consenter knows the password, or even if one exists. This fact is critical to assessing the person's authority but unknown to the officer. While a finding of apparent authority allows for officer error, there is no room for error where the expectation of privacy is so high and the burden on law enforcement is so low.[133] Thus, it is reasonable to require officers to ask one or two more questions before commencing a search that would potentially invade an individual's privacy without jus-

129. *Id.* at 718 (citing *Gourde*, 440 F.3d at 1077).

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

130. *See* Lawrence v. Texas, 539 U.S. 558, 564-565 (2003) (referencing the emphasis placed on the bedroom in Griswold v. Connecticut in discussing individuals' privacy interests); *Kyllo*, 533 U.S. at 34 (recognizing the interior of the home, as the most protected); *Griswold*, 381 U.S. at 485 (characterizing the marital bedroom as a "sacred precinct").

131. *Andrus*, 483 F.3d at 719.

132. *Id.* at 716-17 (citing *Rodriguez*, 497 U.S. at 188).

133. *Id.* at 716 (citing Georgia v. Randolph, 547 U.S. 103, 126 (2006)).

tification. Specifically, the officer should ask at least one question about the existence of a password.

Passwords are so commonplace that it is not unreasonable to require that a reasonable officer ask about them. This is especially true where, as in *Andrus*, a forensic computer expert is conducting the search.[134] Law enforcement officers, particularly those employed as forensic computer experts, cannot ignore circumstances known to the average layperson. Officers cannot assess authority to consent to a search without the facts necessary to make that determination. Even though apparent authority allows for officer mistakes, a computer search premised on third-party consent without inquiry into a person's knowledge of a password is unreasonable because the officer has not made a reasonable inquiry into the consenter's authority.[135]

B. Consequences of the *Andrus* holding

As a consequence of the *Andrus* holding, the expectation of privacy an individual has in his computer and the information on it is eroded. EnCase enables law enforcement to bypass the password protection a user puts in place to ensure the privacy of his or her information. As a result of this holding, occasionally letting your roommate use your computer or borrow clothes can be enough to give her apparent authority to consent to a search of your computer, even if she does not have the password. For example, your roommate might enjoy full access to your room, your closet, or your desk. You might let her use your computer to check her e-mail or print a document. Based on apparent authority, an inquiry that merely scratches the surface on access to the room and use of the computer allows your roommate to consent to a search of your computer in this situation. Because EnCase and similar technology allows officers to search a computer's contents without even turning it on, your efforts to protect your privacy by creating a user profile or setting a password become futile.

On appeal the Tenth Circuit clarified its holding in *Andrus* by stating that questions regarding EnCase's capability to detect password protection or user profiles on home computers were not presented to the court.[136] By avoiding the issues surrounding officers' use of EnCase, *An-*

134. *Id.* at 713. Becoming a proficient user of EnCase Forensic takes about 18 months and costs about $4,000 in classes. Ryan Blitstein, *Part III: U.S. Targets Terrorists as Online Thieves Run Amok*, San Jose Mercury News, Nov. 12, 2007, *available at* http://www.mercurynews.com/bizreports/ci_7442979. Training "forensic cybercops" costs the government over $10,000, plus travel and time off. *Id.*

135. *See Salinas-Cano*, 959 F.2d at 865-66 (determining officers' belief in apartment owner's authority to consent to search of defendant's suitcase to be unreasonable where police failed to inquire into apartment owner's use of or control over the suitcase).

136. *Andrus*, 499 F.3d at 1162-63.

drus is likely to create confusion for law enforcement and future cases, at least in the context of third-party consent. For example, officers seeking the consent of a third party to search a computer could be uncertain about the questions they need to ask before they have a valid consent. The most likely circumstance is that officers will make a minimal inquiry into the consenter's computer access and use. Then, a defense attorney who has read *Andrus* will move to suppress the evidence from the search and support the motion with the implications from *Andrus*. Specifically, this attorney will provide the information necessary to make the presence of computer passwords a judicially noted fact.[137] This attorney will argue that a computer search grounded on third-party consent that does not take the existence of passwords into account is unreasonable. The defense attorney might succeed, especially given the support she will find in decisions from other circuits.

Other circuits have placed greater importance on the presence of a computer's password protection. For instance, the court in *United States v. Smith*[138] concluded that, where the computer was located in a common area and the defendant had not password-protected his files, his girlfriend had authority to consent to a search of the computer.[139] In another case, a federal district court judge held that requiring a defendant in a child pornography case to provide his computer password in response to a grand jury subpoena would be a violation of his Fifth Amendment right against self-incrimination.[140] In *Trulock v. Freeh*,[141]

137. *Andrus*, 483 F.3d at 721.

138. United States v. Smith, 27 F. Supp. 2d 1111 (C.D. Ill. 1998).

139. *Id.* at 1115-16.

140. In re Boucher, No. 2:06-mj-91, 2007 U.S. Dist. WL 4246473, at *3 (D. Vt. Nov. 29, 2007), *rev'd*, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009). A Customs and Border Protection Officer opened Boucher's laptop during a border search and was able to access files showing child pornography without entering a password. *Id.* at *1. Boucher waived his Miranda rights and spoke with agents. *Id*. Agents shut down the laptop and created a mirror image of its contents but were not able to access the drive containing the pornography after shutting it down. *Id.* at *2. The government's only hope to unlock the drive was to use an automated system which guesses passwords, which could take years. *Id.* The magistrate judge found that requiring Boucher to enter the password would be forcing him to produce incriminating evidence because he "would be compelled to produce his thoughts and the contents of his mind." *Id.* at *3-4. The judge also rejected the government's suggestions to have Boucher enter the password without anyone seeing it or to exclude his entering the password from evidence. *Boucher*, 2007 WL 4246473, at *4-5. On appeal, the district court reversed the magistrate judge's decision, holding, "the contents of the laptop were voluntarily prepared or compiled and are not compiled, and therefore do not enjoy Fifth Amendment protection." *Boucher*, 2009 WL 424718 at *2. The district court stated that Boucher had no act of production privilege and ordered him to provide an unencrypted version of the drive the agent viewed. *Id.* at *4. Further, the court ordered that the government cannot use "Boucher's act of production to authenticate the unencrypted Z drive or its contents either before a grand jury or a petit jury." *Id.* Boucher's attorney has filed an appeal to the Second Circuit. Declan McCullagh, *Judge Orders Defen-*

the defendant's live-in girlfriend, who had joint access to the computer's hard drive, had authority to consent to a general search of the computer, but not the defendant's password-protected files.[142] The court compared the password-protected files to a locked footlocker inside a bedroom.[143] Following *Trulock*, the court in *United States v. Buckner*[144] took the absence of any indication of password protection into account in finding that the defendant's wife's consent to search the computer was valid, despite the fact that she did not have actual authority.[145] In that case, officers used forensic software to create a mirror image[146] of the computer's hard drive.[147] The court was careful to note that it did not hold that "officers could rely on 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."[148]

The court in *Buckner* appears to attempt to close the loophole left open by *Andrus*. Under *Andrus*, officers can avoid discovery of passwords and user profiles by using EnCase software to search. Officers can assure the validity of the third-party consent search by limiting the "facts available" at the time the search is commenced.[149] As long as the "facts available" are enough to amount to apparent authority, any other facts that might diminish that authority are inconsequential, because the search will be upheld under the exception.[150] This is not to say that law enforcement is inclined to deliberately avoid password protection on home computers.[151] However, agencies may rely on the holding in *Andrus* and implement or continue search procedures that do not check for passwords. In some instances, this will result in the invasion of individ-

---

dant to Decrypt PGP-Protected Laptop, CNET NEWS, Feb. 26, 2009, http://news.cnet.com/8301-13578_3-10172866-38.html.

141. 275 F.3d 391 (4th Cir. 2001).

142. *Id.* at 403. The computer was located inside their shared bedroom. *Id.*

143. *Id.* at 403 (citing United States v. Block, 590 F.2d 535, 541 (4th Cir. 1978)).

144. United States v. Buckner, 473 F.3d 551 (4th Cir. 2007).

145. *Id.* at 555-56. The court also took into consideration that the computer was located in a common living area, the computer was on, and officers had been told that fraudulent activity had been conducted from that computer using accounts opened in the wife's name. *Id.* at 555.

146. EnCase has the capability to create mirror images, or forensic copies of hard drives. The copies are mirror images because they are copies of all information on the drive, including deleted files. *See supra* text accompanying notes 34-39.

147. *Buckner*, 473 F.3d at 553.

148. *Id.* at 555 n.3. Defendant did not contend that the officers deliberately used the software to avoid discovery of existing passwords. *Id.* at 552 n.1.

149. *Andrus*, 483 F.3d at 716-17 (citing *Rodriguez*, 497 U.S. at 188).

150. *Id.* at 716 (citing Georgia v. Randolph, 547 U.S. 103, 126 (2006)).

151. However, defendants will almost certainly argue that this is the case. This might be particularly true in the Fourth Circuit, where the court commented that the defendant did not make this argument. *Buckner*, 473 F.3d at 552 n.1.

uals' right to privacy in the information stored on their computers. In other cases, law enforcement's reliance on *Andrus* could be to its detriment and these searches will be held invalid. At the very least, *Andrus* provides defendants with an argument to suppress the evidence recovered from the search. In prosecutions for serious crimes such as child pornography, the consequences of an invalid search can be devastating.

C. Alternative disposition of *Andrus*

The dissent's analysis in *Andrus* is correct and the rule set forth by the dissenting judge should be followed. The dissent articulated the rule as follows:

> [I]n consent-based, warrantless computer searches, law enforcement personnel [must] inquire or otherwise check for the presence of password protection and, if a password is present, inquire about the consenter's knowledge of that password and joint access to the computer.[152]

To elaborate on this rule, officers should be required to ask the consenting party if they know whether a password exists on the computer and if they possess the password before beginning a search using EnCase or similar forensic software. An alternative would be for officers to rely on the third-party consent to image the hard drive, but not to search its contents without a warrant or consent by the owner.[153]

This rule would be in accord with the principles behind the third-party consent exception set forth in *United States v. Matlock*.[154] Requiring officers to check for the presence of a password and the consenter's knowledge of that password ensures that the party consenting to the search has joint access and control. Though the law allows for reasonable error by law enforcement in assessing the apparent authority of a party to search, this rule increases the validity of computer searches based on third-party consent. In addition, the rule enhances individuals' interests in the privacy of the information contained on their computer's hard drive. This rule is more congruous with the comparison of computers to other objects and containers that command a high expectation of privacy. Computer users are presumed to have a high expectation of privacy as well as a desire to protect their most "intimate information," so courts should do what is within their power to protect these inter-

152. *Andrus*, 483 F.3d at 725 (McKay, J., dissenting).

153. For a proposal on handling off-site searches of imaged hard drives, *see* Brenner & Frederiksen *supra* note 35, at 75 (arguing against a blanket prohibition of off-site hard drive image searches). The authors suggest that agents create two mirror images of the hard drive immediately –one copy to search, and one sealed copy to provide to the defendant, his counsel, or his experts. *Id.* at 79.

154. 415 U.S. 164 (1974).

ests.[155] Courts can afford individuals this protection by requiring law enforcement to make a reasonable inquiry into the measures an individual has taken to protect the information on her computer. Further, this rule affords password protection the significance it has been given in other cases involving third-party consent searches of computers.[156] Because it is more consistent with cases from other circuits and Fourth Amendment analysis, less confusion would likely follow this disposition.

Moreover, the court could have come to this disposition by using a balancing test. The individual's privacy interest in the information stored on her computer and right to be free from unreasonable searches can be balanced against the burden imposed on governmental interests by requiring law enforcement to check for passwords before using EnCase to search a computer.[157] This type of balancing has been used to analyze the reasonableness of "stop and frisk" seizures under the Fourth Amendment.[158]

The majority in *Andrus* concedes that the burden on the officers in this case was minimal.[159] In fact, where the third party is in front of officers, he is likely answering a number of questions. Asking a few additional questions would pose a minimal burden to both parties in the majority of cases. For example, after determining the location of the computer within the residence, the officer could ask the consenter if he uses the computer. This question could be followed by, "Is there a password on the computer?" If the consenter answers yes, the officer would ask, "Do you know the password?" Asking just these few questions ascertains the extent of the consenting party's access and control over the computer. A person who answers these questions in the affirmative likely has actual authority to consent to the search. Even if they do not have actual authority, the reasonableness of the officer's belief that the consenter has apparent authority is validated.

---

155. *Andrus*, 483 F.3d at 718.

156. *See* United States v. Buckner, 473 F.3d 551 (4th Cir. 2007); Trulock v. Freeh, 275 F.3d 391 (4th Cir. 2001); United States v. Smith, 27 F. Supp. 2d 1111 (C.D. Ill. 1998).

157. As noted by the dissent, the burden on law enforcement was minimal. *Andrus*, 483 F.3d at 724 (McKay, J., dissenting).

158. *See* Brown v. Texas, 443 U.S. 47, 52-53 (1979) (balancing public interest and an individual's right to personal security and privacy in invalidating a statute that criminalized refusing to provide a name and address to an officer who requested it); Terry v. Ohio, 392 U.S. 1, 20 (1968) (stating that the reasonableness of seizures that are less intrusive than a traditional arrest depends "on a balance between the public interest and the individual's right to personal security free from arbitrary interference by law officers."). "Consideration of the constitutionality of such seizures involves a weighing of the gravity of the public concerns served by the seizure, the degree to which the seizure advances the public interest, and the severity of the interference with individual liberty." *Brown*, 443 U.S. at 50-51 (citing United States v. Brignoni-Ponce, 422 U.S. 873, 878 (1975)).

159. *Andrus*, 483 F.3d at 720.

Similarly, while creating a mirror image of the hard drive and seeking a warrant before searching it imposes a greater burden on law enforcement, the government's case is only strengthened by these efforts. Enhancing the evidence against the defendant reduces litigation over preliminary matters and allows the parties to discuss resolution of the merits sooner. Furthermore, the computer user's interest in the privacy of the information stored on the computer is preserved and the burden on law enforcement is minimal.

This is not to say that EnCase should not be used in computer searches. In fact, EnCase can potentially help preserve individuals' expectations of privacy in the information stored on their computers. EnCase allows investigators to limit the files acquired to those relevant to the case and all information related to those files.[160] By automating the search, files unrelated to the case are kept from the eyes of the investigator in most instances. Instead of going through a user's folder full of pictures, some related to the case and others not, EnCase allows the investigator to automatically search and analyze specific documents and document types using complex criteria.[161] Thus, EnCase automatically limits the scope of the search without a manual, human eye going through the user's files.[162] In addition, EnCase creates a mirror image of the hard drive that is read-only, or cannot be changed.[163] The fact that it can create this mirror image without turning the computer on is actually a benefit. If officers were required to turn the computer on or off before imaging the hard drive, evidence would be destroyed.[164] This fea-

160. Guidance Software, EnCase Field Intelligence Model, *supra* note 34, at 2. *See also* Brenner & Frederiksen *supra* note 35, at 95 (analogizing searching with computer forensic software to searching for contraband with a drug-sniffing dog).

161. Guidance Software, EnCase Forensic LE, *supra* note 32, at 2.

162. Ironically, the Tenth Circuit has been somewhat restrictive in limiting the scope of computer searches. *See* United States. v. Walser, 275 F.3d 981, 986 (10th Cir. 2001) ("Because computers can hold so much information touching on many different areas of a person's life, there is greater potential for the 'intermingling' of documents and a consequent invasion of privacy when police execute a search for evidence on a computer."); United States v. Carey, 172 F.3d 1268, 1273-75 (10th Cir. 1999) (finding that officers exceeded the scope of a search for evidence where, upon discovering an image of child pornography, officers "abandoned the search" and instead searched for child pornography for five hours). *But see* United States v. Slanina, 283 F.3d 670, 680 (5th Cir. 2002) (holding that once a warrantless search of a portion of a computer and zip disk had been justified, the comprehensive search of the other contents of the computer and zip disk was valid because defendant no longer retained any reasonable expectation of privacy in the remaining contents).

163. Guidance Software, EnCase Forensic LE, *supra* note 32, at 2.

164. Starting a Microsoft Windows system destroys "more than 4,000,000 characters of evidence, and the spoliation will be far greater if the system is used to run any programs." Brenner & Frederiksen *supra* note 35, at 66 (describing how inadvertent spoliation can occur when searching computers for evidence). The unfortunate circumstances for law enforcement officers in the *Boucher* case illustrate this potential loss of evidence on a greater scale. *Boucher*, 2007 WL 4246473, at *2 (holding that Boucher could not be forced to reveal

ture helps to protect the integrity of the searches and the admissibility of the evidence recovered. However, when EnCase is used to search a computer without a warrant or valid consent, the result is an unreasonable search.

VI. CONCLUSION

In conclusion, the court in *Andrus* erred in finding that the officers were not required to inquire about or check for password protection before using EnCase to search a computer where the search was premised on third-party consent. This finding runs contrary to established principles of the third-party consent exception and controverts the analysis employed by the court in analyzing the expectations of privacy in computer data. A better disposition of this case is set forth in the dissenting opinion.

The dissent in *Andrus* correctly addressed the issue of the officers' use of EnCase without sufficient inquiry into Dr. Andrus' use of his son's computer. The rule set forth in this opinion should be followed. Before beginning a search using EnCase or similar forensic software, officers should be required to ask the consenting party whether a password exists on the computer and if they know the password. Officers could also consider relying on the third-party consent in imaging the hard drive and waiting to search the contents until they obtain the owner's consent or a warrant. This rule is in agreement with the analysis of expectations of privacy associated with computers, particularly where password protection is present, as well as the reasoning behind the third-party consent exception. Because the majority's holding creates confusion for law enforcement agencies and courts, it is likely to be questioned in the future.

---

the password to the computer after agents lost access to the drive by turning the computer off). For more details about the *Boucher* case and the appeal, *see supra* note 140.