Denver Law Review

Volume 85
Issue 3 *Tenth Circuit Surveys*

Article 9

January 2008

The Fourth Amendment, Password-Protected Computer Files and Third Party Consent Searches: The Tenth Circuit Broadens the Scope of Warrantless Searches

Michael Smith

The Fourth Amendment, Password-Protected Computer Files and Third Party Consent Searches: The Tenth Circuit Broadens the Scope of Warrantless Searches

THE FOURTH AMENDMENT, PASSWORD-PROTECTED COMPUTER FILES AND THIRD PARTY CONSENT SEARCHES: THE TENTH CIRCUIT BROADENS THE SCOPE OF WARRANTLESS SEARCHES

INTRODUCTION

When ninety-one-year-old Dr. Bailey Andrus opened the door in his pajamas, he was greeted by state and federal law enforcement agents.[1] The agents had been investigating a company called RegPay, which provided, among other things, access to Internet sites displaying child pornography.[2] During the investigation the agents obtained a list of RegPay's customers, and on this list was the name of fifty-one-year-old Ray Andrus, Dr. Andrus's son.[3]

Eight months into the investigation, agents "believed they did not have enough information to obtain a search warrant . . . [and] attempted to gather more information by doing a knock and talk interview with the hope of being able to conduct a consent search."[4] Ray Andrus was at work when the agents knocked on the door.[5] The agents obtained consent from Andrus's father and—using high-tech computer forensics software—quickly collected information from Andrus's computer.[6] The agents used a software program that copied Andrus's hard-drive without first determining whether any of the files were password-protected.[7] So without a search warrant, and without Andrus being present, government agents used high-tech equipment to search his password-protected computer files.

The Fourth Amendment of the United States Constitution declares that:

> 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.[8]

---

1. United States v. Andrus, 483 F.3d 711, 713 (10th Cir. 2007), *petition for cert. filed*, No. 07-0753 (U.S. Nov. 21, 2007).
2. *Id.*
3. *Id.*
4. *Id.* (internal quotation marks omitted).
5. *Id.*
6. *Id.*
7. *Id.* at 713-14.
8. U.S. CONST. amend. IV.

The key question in *United States v. Andrus* was whether it was *reasonable* for the government to conduct a search in the manner described above.

The text of the Fourth Amendment has two clauses: "one speaking to unreasonable searches and seizures, and the other discussing the requirements for the issuance of warrants."[9] Over the two-hundred plus years since the drafting of the amendment, the Court has struggled to develop a coherent approach to its interpretation of these two clauses. The result is what one commentator referred to as a "vast jumble of judicial pronouncements that is not merely complex and contradictory, but often perverse."[10] Or, even more bluntly, "[t]he Fourth Amendment today is an embarrassment."[11]

In spite of past difficulties with interpretation, courts have developed longstanding rules and doctrines that guide police in the conduct of searches and seizures. However, there are significant new challenges facing the courts in determining what constitutes a search and a seizure of data from a computer. Thus, not only did Dr. Andrus open the door allowing agents to enter his home, but he also unknowingly opened another door into the extraordinarily important legal issue of searches and seizures in the digital age.

This comment will discuss and analyze the issues implicated in *Andrus* in three parts. Part I will trace the historical development of Fourth Amendment jurisprudence. It has been argued that modern approaches to understanding this area of the law are insufficient.[12] The goal in this Part is to identify patterns and trends that will provide a context for understanding *Andrus*. Part II includes a detailed presentation of the Tenth Circuit's holding in *Andrus*, including the dissent. Part III will include an in-depth analysis of the Tenth Circuit's holding in *Andrus* in light of the background cases and history of the Fourth Amendment. Part III also concludes that the outcome could have been different had Andrus invoked the Court's holding in *Kyllo v. United States*.[13]

I. BACKGROUND

One of the most abiding concerns in the American experience has been the tension between individual freedoms and the security of its people. The Founding Fathers were keenly aware of this tension, and, since its birth over two-hundred years ago, the Fourth Amendment has served

9. Sam Kamin, *The Private is Public: The Relevance of Private Actors in Defining the Fourth Amendment*, 46 B.C. L. REV. 83, 88 (2004).

10. AKHIL REED AMAR, THE CONSTITUTION AND CRIMINAL PROCEDURE 1 (1997).

11. *Id.* at 1.

12. *See id.* at 2 ("[S]cholars ponder every nuance of the latest Supreme Court case but seem unconcerned about the amendment's text, unaware of its history, and at times oblivious or hostile to the common sense of common people.").

13. 533 U.S. 27, 40 (2001).

as a primary check on the power a government can exercise over its citizens. These concerns have remained at the center of the national debate as the tensions between freedom and security continue to make their way into the news headlines of the day.

A. Historical Development of the Fourth Amendment

1. Eighteenth-Century Origins of the Fourth Amendment

The framers of the Constitution and Bill of Rights were united in their concerns about the power of the newly formed federal government. It was their familiarity with the expansive powers of the King of England that led to the Fourth Amendment.[14] While the Fourth Amendment "was prompted by complaints pressed during the Constitution's ratification . . . its real source . . . [was] a trio of famous cases from the 1760s, two in England and one in the colonies."[15] The two English cases involved "authors of political pamphlets critical of the King's ministers."[16] The authors of the pamphlets "suffered the ransacking of their homes and the seizure of all their books and papers . . . ."[17] The authors sued government officials and won on the holding that the government had trespassed on their property.[18]

More importantly, however, a historic opinion—written by Lord Cramden—got the attention of the American colonists.[19] Lord Cramden condemned the practice of "general warrants," which allowed the King's officials to search and seize private property on a mere suspicion, and did not require the officials to make any attempt to identify with specificity the materials that were the subject of the search.[20] Essentially, under British law the King's officials could enter a person's home on mere suspicion and search anything they deemed necessary to determine if there was any wrongdoing.[21] It was this unfettered government power that most concerned Lord Cramden. He announced that "[i]f such a power is truly invested in a secretary of state, and he can delegate this power, it certainly may affect the person and property of every man in this kingdom, and is *totally subversive of the liberty of the subject*."[22]

During this time there were widespread concerns of illegal smuggling in the colonies resulting largely from the strict controls on colonist

---

14. *See* William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393, 396-97 (1995).
15. *Id.* at 396.
16. *Id.* at 397. One of the authors was John Wilkes, a member of English Parliament who had secretly written a pamphlet called The North Briton. *Id.* at 398.
17. *Id.* at 397.
18. *Id.* at 397-98.
19. *Id.* at 399.
20. *Id.*
21. *Id.*
22. *Id.* (emphasis added).

trade activities.[23] Predictably, officials wanted to squelch this activity and thus relied on British law that allowed officials to "enter, and go into any House, Shop, Cellar, Warehouse or Room, or other Place, and in Case of Resistance, to break open Doors, Chests, Trunks and other Package[s] . . . ."[24] Consequently, colonists were targeted in an attempt to find evidence of smuggling, and a lawsuit was filed in Boston to challenge the validity of these laws.[25] The thrust of the argument was that should these so-called "writs of assistance" be upheld, they would "totally annihilate" the long-standing principle that "[a] man's house is his castle . . . ."[26] The court held that the searches were valid,[27] but the larger point had been made: the colonists were displeased with the broad search and seizure powers of the government and they would continue to challenge them.

With this background, it is not surprising that the framers of the United States Constitution sought to restrict the power of the government to invade the homes of its citizens. Drawing upon the experiences of the colonies and nascent states, the Fourth Amendment text was adopted "as a specific response to a specific grievance that had arisen in a specific historical context and had been shaped by a specific vulnerability in the protections afforded by common-law arrest and search authority."[28]

2. The United States Supreme Court's Interpretation of the Fourth Amendment and the Warrant Requirement

The Court appeared to establish early that the amendment was not simply a tool to limit the powers of the government, but that it essentially stood for the right of individuals to be free from improper government invasions into their personal lives. An early example of this perspective can be found in the 1886 case of *Boyd v. United States*.[29] In *Boyd*, Justice Bradley and the Court declared that "[i]t is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the *invasion of his indefeasible right of personal security, personal liberty and private property*" that forms the underlying concern for regulating the government's power to search.[30]

The first question courts ask when faced with a search and seizure issue is whether the Fourth Amendment is even implicated. It then be-

23. *Id.* at 404-05.
24. *Id.* at 404.
25. *Id.* at 405-06. John Otis represented the colonists in their attempt to eliminate the use of the writs of assistance by the British government. Even though Otis lost the case, his challenge of the writs prompted John Adams to later say that "Otis had, in effect, fired the first shot of the Revolution." *Id.* at 406.
26. *Id.*
27. *Id.*
28. Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 723 (1999).
29. 116 U.S. 616 (1886).
30. *Id.* at 630 (emphasis added).

comes important to understand what has to occur to even trigger an analysis of the constitutionality of a particular search or seizure. Generally, there are two requirements. First, there must actually be a "search" of something deemed to be private, and second, the search must stem from government action.[31] Once a search has occurred by a government actor, the analysis then turns to whether the search violated the Constitution.

Generally, if a search was conducted without a warrant then the search is deemed "per se unreasonable."[32] In order to get a warrant, government agents must persuade a judge that the evidence sought will likely result in an arrest.[33] In analyzing the warrant requirement of the Fourth Amendment, courts place great emphasis on whether a warrant was obtained prior to conducting the search. Some commentators have questioned this rule on the basis that the text of the Fourth Amendment does not have a "warrant requirement," but only requires, in the cases where a warrant is obtained, that the search be reasonable.[34] Nevertheless, the Court has held that "[t]he Fourth Amendment proscribes all unreasonable searches and seizures, and it is a cardinal principle that [warrantless searches] . . . are *per se* unreasonable . . . subject only to a few specifically established and well delineated exceptions."[35]

3. Warrantless Searches: Exceptions to the Per Se Rule

The Court has carved out several scenarios where the government can attempt to justify a warrantless search after the search is completed. Whereas the per se unreasonable rule provides for judicial review of reasonableness *prior* to the search, the warrantless search exceptions provide judicial review *after* the search is conducted to determine whether it was reasonable. If a court—after a search has been completed—determines that the government violated the Fourth Amendment, then the evidence that was obtained in the illegal search is inadmissible in criminal proceedings.[36] Even if a defendant's guilt is obvious, if the police did not follow constitutional standards the evidence cannot be used against the defendant at trial.[37] Consequently, this "exclusionary rule" compels

31. Kyllo v. United States, 533 U.S. 27, 32-33 (2001) (explaining that "a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.").

32. DANIEL SOLOVE, THE DIGITAL PERSON 189 (2004).

33. *Id.*

34. AMAR, *supra* note 10, at 9-10 (stating that "[w]e need to read the amendment's words and take them seriously: they do not require warrants, probable cause, or exclusion of evidence, but they do require that all searches and seizures be reasonable.").

35. Mincey v. Arizona, 437 U.S. 385, 390 (1978).

36. 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 1.6 186-87 (4th ed. 2004).

37. *Id.*

police to conduct warrantless searches in a constitutionally valid manner.[38]

The Court has upheld several instances of warrantless searches.[39] Some examples of valid warrantless searches include: searches prior to arrest,[40] searches as a result of emergency situations,[41] and searches of items in "plain view."[42] However, the Court has validated another type of warrantless search that was at issue in *Andrus*, which involves consent searches.[43] The consent obtained in *Andrus* was from a third party.[44] Therefore, the Court's approach to third party consent should be considered in more depth.

4. Consent Search Requirements

The right to be free from unreasonable searches from the government can be waived.[45] The Court has further held that knowledge of the right to refuse to consent to a search is no hindrance to the legitimacy of a consent search.[46] That is, the police do not have to tell a person that he has the right to refuse to consent to a warrantless search. This is different from other constitutional rights that cannot be waived and require government officials to inform citizens of their rights.[47] When government agents find it necessary, they may ask for consent to search private property, and, as long as the consent is voluntary,[48] the search is valid under the Fourth Amendment.

---

38. *Id.* § 1.1(f) at 21-22.

39. 36 GEO. L.J. ANN. REV. CRIM. PROC. 3, 38 (2007) (listing thirteen scenarios where "certain kinds of searches and seizures are valid as exceptions to the probable cause and warrant requirements.").

40. *Id.* at 59-62.

41. *Id.* at 73-82.

42. *Id.* at 68-72.

43. 4 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 8.1 at 4-8 (4th ed. 2004).

44. United States v. Andrus, 483 F.3d 711, 720 (10th Cir. 2007), *petition for cert. filed*, No. 07-0753 (U.S. Nov. 21, 2007).

45. LAFAVE, *supra* note 36, § 44, § 8.1(a) at 8-9; *see also* Schneckloth v. Bustamante, 412 U.S. 218, 227 (1973) (stating that "[i]n situations where the police have some evidence of illicit activity, but lack probable cause to arrest or search, a search authorized by a valid consent may be the only means of obtaining important and reliable evidence.").

46. *Schneckloth*, 412 U.S. at 231-32 (reasoning that "it would be thoroughly impractical to impose on the normal consent search the detailed requirements of an effective warning. Consent searches are part of the standard investigatory techniques of law enforcement agencies. They normally occur on the highway, or in a person's home or office, and under informal and unstructured conditions."). *But see* Ohio v. Robinette, 519 U.S. 33, 39 (1996) (holding that consent is to be determined by the totality of the circumstances; thus, if a person had already been told they could refuse, then this information could be considered in the analysis of whether the subsequent consent search was reasonable under the circumstances).

47. *See* LAFAVE, *supra* note 36, at § 44, § 8.1(a) at 8-9.

48. Bumper v. North Carolina, 391 U.S. 543, 546-48 (1968) (holding that when consent is based on an erroneous claim by government officials that they do, in fact, have a search warrant, the consent is invalid thus rendering the search unconstitutional).

The Court has also held that consent can be obtained from third parties. For example, in *United States v. Matlock*,[49] the Court declared:

> [W]hen the prosecution seeks to justify a warrantless search by proof of voluntary consent, it is not limited to proof that consent was given by the defendant, but may show that permission to search was obtained from a third party who possessed common authority over or other sufficient relationship to the premises or effects sought to be inspected.[50]

The reasoning of the Court in *Matlock* is premised on the third party having actual authority to consent to the search. For example, when a police officer gets permission to search a house from a roommate—rather than the actual target of the search—the search will be valid as long as the roommate possesses "common authority over or other sufficient relationship" to the house.[51]

But what if police later learn that the third party did not possess the requisite authority to consent? Justice Scalia—writing for the Court in *Illinois v. Rodriguez*[52]—stated that the analysis will not turn on whether the police officer was right about the third party's authority, but whether his presumption of authority was reasonable.[53] So, if a police officer reasonably believes that the person providing the consent meets the requirements set forth in *Matlock*, then whether he actually does or not is irrelevant. Justice Scalia reasoned that police officers will have to make decisions based on the facts they are provided in any given circumstance; therefore, if the judgment is reasonable given the information they are provided, then that should not change the underlying validity of the search if it is later learned that the information was false or inaccurate.[54]

Allowing the government to search private homes and property under the authority of third party consent appears to give broad powers to the government. Recently, however, the Court narrowed the rules of consent searches when it held that third party consent is invalid when the person that is the target of the search is present, *and* they object to the search.[55] For example, if the police want to search the house of a husband and wife because they believe the husband is engaged in some illegal activities, the wife's consent is invalid if the husband is both present and he objects to the search.[56]

---

49. 415 U.S. 164 (1974).
50. *Id.* at 171.
51. *Id.*
52. 497 U.S. 177 (1990).
53. *Id.* at 185.
54. *Id.* at 185-86.
55. *See* Georgia v. Randolph, 547 U.S. 103, 120 (2006).
56. *See id.* at 125.

In sum, the Fourth Amendment requires that the government obtain a warrant based on probable cause to validly search a person's property. Moreover, the warrant cannot be general, but must specify "the place to be searched, and the persons or things to be seized."[57] If the government has not obtained a warrant, then the search is considered per se unreasonable unless the government can justify the search under one of the recognized exceptions for warrantless searches.[58] Of particular importance for this comment is the third party consent exception because this is what the government obtained from Andrus's ninety-one-year-old father.[59]

B. Emerging Technologies and Reasonable Expectations of Privacy

The Fourth Amendment was originally applied to searches and seizures of tangible items.[60] This perspective was grounded in the text of the amendment, which lists items such as "persons, houses, papers, and effects . . . ."[61] Historically, this made sense, for as Justice Brandeis observed, "[f]orce and violence were then the only means known to man by which a government could . . . secure possession of his papers and other articles incident to his private life . . . ."[62] Consequently, the Court took a narrow approach to the determination of whether a particular search implicated the Fourth Amendment. Predictably, this approach was put to the test as new technologies developed allowing the government to gain access to private information without resorting to "force and violence."

1. From *Olmstead* to *Katz* and Reasonable Expectations of Privacy

In *Olmstead v. United States*,[63] the United States charged over seventy defendants with violating the National Prohibition Act.[64] Over a period of several months government agents listened to phone conversations confirming the illegal activities of the defendants.[65] The agents had conducted wiretapping "without trespass upon any property of the defendants."[66] The wiretap technology thus allowed agents to get information without resorting to "force and violence." Accordingly, invoking the literal language and historical origins of the text, Chief Justice Taft—writing for the majority—declared that the Fourth Amendment "does not forbid what was done [in this case]. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing

57. U.S. CONST. amend IV.
58. *See* Kyllo v. United States, 533 U.S. 27, 31 (2001).
59. United States v. Andrus, 483 F.3d 711, 720 (10th Cir. 2007), *petition for cert. filed*, No. 07-0753 (U.S. Nov. 21, 2007).
60. Orin Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 533 (2005).
61. U.S. CONST. amend. IV.
62. Olmstead v. United States, 277 U.S. 438, 473 (1928) (Brandeis, J., dissenting).
63. *Id.* at 455-56.
64. *Id*
65. *Id.* at 457.
66. *Id.*

and that only. There was no entry of the houses or offices of the defendants."[67]

Olmstead appears to adhere to the text and original meaning of the Fourth Amendment.[68] However, Justice Brandeis dissent foreshadowed the underlying flaws in *Olmstead* by observing that "[t]ime works changes, brings into existence new conditions and purposes. Therefore a principal to be vital must be capable of wider application than the mischief which gave it birth."[69]

Almost forty years after *Olmstead*, the Court addressed the issue of whether bugging a phone booth implicated a search under the Fourth Amendment.[70] The government suspected defendant Katz of participating in illegal wagering over wire communications and consequently installed a bugging device into the phone booth where he was believed to make the calls.[71] At trial, the government presented the evidence obtained from the calls and won a conviction.[72] Katz objected to the admissibility of the evidence, arguing that it was obtained in violation of the Fourth Amendment.[73]

Understandably, both the district court and the appellate court relied on *Olmstead* in their determinations that the bugging of the phone booth did not implicate the Fourth Amendment because there was no physical breach.[74] Moreover, it was reasonable to infer from the Court's past holdings that the issue would turn on whether a phone booth was a "constitutionally protected area."[75]

However, writing for the Court, Justice Stewart explained that

> [b]ecause of the misleading way the issues have been formulated, the parties have attached great significance to the characterization of the telephone booth from which the petitioner placed his calls. The petitioner has strenuously argued that the booth was a "constitutionally protected area." The Government has maintained with equal vigor that it was not. But this effort to decide whether or not a given "area," viewed in the abstract, is "constitutionally protected" deflects attention from the problem presented by this case.[76]

With the context of the issue properly situated, Justice Stewart then delivered a fatal blow to *Olmstead* by announcing that "the Fourth

---

67. *Id.* at 464.
68. *See* Kamin, *supra* note 9, at 94 (stating that "[a]s a reading of the text, this interpretation of the Fourth Amendment is almost entirely unassailable.").
69. *Olmstead*, 277 U.S. at 472-73 (Brandeis, J., dissenting).
70. Katz v. United States, 389 U.S. 347, 349 (1967).
71. *Id.* at 348-49.
72. *Id.* at 348.
73. *Id.*
74. *See id.* at 348-49.
75. *See id.* at 350.
76. *Id.* at 351.

Amendment *protects people, not places*."[77] Consequently, a new approach to Fourth Amendment jurisprudence was established.

Katz emphasized the expectations of privacy manifested by the individual. Specifically, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[78] Knowledge of whether an individual has a reasonable expectation of privacy is thus what determines if the Fourth Amendment is implicated. In *Katz*, the defendant was in a public place and exhibited a reasonable expectation because he closed the door to the phone booth, manifesting a desire for privacy.[79]

Katz provides the guidelines for a court to determine whether the Fourth Amendment has been implicated in a search. Since *Katz*, the Court has interpreted a reasonable expectation of privacy to consist of a manifested subjective expectation of privacy by the individual that society would recognize as objectively reasonable.[80] Thus, the individual has to demonstrate that he expects privacy *and* society has to accept that expectation as reasonable.

2. Issues in Determining Reasonable Expectations of Privacy

Predictably, applying *Katz* presents questions such as how a court determines whether a person has an expectation of privacy. Or, how does a person actually manifest that he has an expectation of privacy that society would find reasonable? In *United States v. Miller*,[81] the Court held that when a person voluntarily turns over private financial information to a bank, the person has thus exhibited that he *does not* have a reasonable expectation of privacy because "[t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[82] Accordingly, there was no search in *Miller* that required Fourth Amendment protection.[83]

In *Smith v. Maryland*,[84] the police had a phone company install a device that recorded all the numbers dialed from Smith's home.[85] Police

77. *Id.* (emphasis added).
78. *Id.*
79. *See id.* at 352 (stating that "one who occupies [the phone booth], shuts the door behind him, and pays the toll . . . is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.").
80. *See* California v. Greenwood, 486 U.S. 35, 39 (1988).
81. 425 U.S. 435 (1976).
82. *Id.* at 443. The Court added that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by [the third party] to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and confidence placed in the third party will not be betrayed. *Id.*
83. *Id.* at 444.
84. 442 U.S. 735 (1979).
85. *Id.* at 737.

had suspected Smith of committing a crime, but had not yet obtained a search warrant.[86] The question was whether it is reasonable to expect that phone numbers dialed from one's home are not being recorded.[87] The Court rejected Smith's argument by doubting "that people in general entertain any actual expectation of privacy in the numbers they dial."[88] The Court invoked *Miller* in concluding that Smith "voluntarily conveyed numerical information to the telephone company . . . [and thus] assumed the risk that the company would reveal to police the numbers he dialed."[89] Read together, *Miller* and *Smith* "establish a general rule that if information is in the hands of third parties, then an individual lacks a reasonable expectation of privacy" thus forfeiting his right to Fourth Amendment protections.[90]

Broadening *Miller* and *Smith*, the Court held that when a person puts his garbage out on the curb of a public street—for the purpose of being picked up by a third party—this will "defeat [the] claim to Fourth Amendment protection" because, even though there may be a subjective expectation of privacy, it is not one society would recognize.[91]

Notably, the Court has also faced issues involving the use of new surveillance devices. In *Dow Chemical Co. v. United States*,[92] the Court held "that the taking of aerial photographs of an industrial plant complex from navigable airspace is not a search prohibited by the Fourth Amendment."[93] More recently, however, the Court held that the use of a thermal imaging device that detects heat inside of buildings was improperly used in determining whether a person was growing marijuana inside his home.[94]

---

86. *Id.*

87. *Id.* at 736.

88. *Id.* at 742.

89. *Id.* at 744.

90. SOLOVE, *supra* note 32, at 201. Professor Solove adds rather ominously that "[g]athering information from third party records is an emerging law enforcement practice with as many potential dangers as the wiretapping in *Olmstead*." *Id.*

91. California v. Greenwood, 486 U.S. 35, 40 (1988) (reasoning that "[i]t is common knowledge that plastic garbage bags left on . . . a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public") (footnotes omitted). *But see id.* at 45-46 (Kennedy, J., dissenting) (protesting that going through someone else's garbage "is contrary to commonly accepted notions of civilized behavior" and that "members of our society will be shocked to learn that the Court . . . [disagrees]"); Georgia v. Randolph, 547 U.S. 103, 131 (2006) (Roberts, C.J., dissenting) (challenging the Court's holding on the grounds that it relies on the interpretation of social norms).

92. 476 U.S. 227 (1986).

93. *Id.* at 239. The Court pointed out, however, that the holding was based partly on the fact that the photographs did not reveal "intimate details," suggesting that had the photographs had been more detailed then the search might have been prohibited. *Id.* at 237-38.

94. Kyllo v. United States, 533 U.S. 27, 40 (2001).

3. *Kyllo v. United States*: The Use of Special Technologies and the Fourth Amendment

Federal agents had suspected that Kyllo was growing marijuana in his home but had not obtained a search warrant.[95] Reasoning that growing marijuana typically requires the use of heat lamps, the agents used a thermal imaging device—which detects levels of heat—that confirmed there was an unusually high level of heat emanating from Kyllo's apartment.[96] Partly on the basis of this information, the agents successfully obtained a search warrant and subsequently found "an indoor growing operation involving more than 100 plants."[97]

After conviction, the Ninth Circuit affirmed the district court because Kyllo "had shown no subjective expectation of privacy because he had made no attempt to conceal the heat escaping from his home . . . ."[98] The Court now had an opportunity to explore the impact of radically changing technologies on existing Fourth Amendment jurisprudence.[99] Writing for the majority, Justice Scalia acknowledged that "[i]t 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."[100] Consequently, the Court would have to establish what—if any—limits should be placed on these powerful new technologies in the hands of government law enforcement agents.[101]

Ultimately, *Kyllo* held that "where . . . the Government uses a device that is not in general public use . . . the surveillance is a 'search' and is presumptively unreasonable without a warrant."[102] Thus, a key principle emerging from *Kyllo* is the importance of technology that "is not in general public use."[103] Interestingly, while *Kyllo* appears to broaden individual freedoms, at least one commentator has suggested that this holding significantly narrows Fourth Amendment protections for individuals.[104] At any rate, *Kyllo* will be critical to lower courts as they confront the challenges of applying old rules to new technologies.

---

95. *Id.* at 29-30.
96. *Id.*
97. *Id.* at 30.
98. *Id.* at 31.
99. *See* Kamin, *supra* note 9, at 114 (suggesting that the Court missed an opportunity because "[i]nstead of confronting the technology question directly . . . the Court looked to the past, principally to *Katz* and *Dow Chemical*, in search of answers").
100. *Kyllo*, 533 U.S. at 33-34.
101. *Id.* at 34.
102. *Id.* at 40.
103. *Id.*
104. *See* Kamin, *supra* note 9, at 117 (predicting that "[o]nce individuals can be fairly charged with an awareness of a technology and its implications . . . they are responsible for protecting themselves from its possible invasions").

II. *UNITED STATES V. ANDRUS*

A. Facts, Holding and Rationale of the Trial Court

As part of a federal investigation into RegPay—a company providing access to Internet sites containing child pornography—federal agents obtained Ray Andrus's name from a list of RegPay's customers.[105] The information included a credit card number and an address, which revealed that Andrus lived with his elderly father.[106] After eight months of surveillance, "agents believed they did not have enough information to obtain a search warrant for the Andrus residence."[107] Consequently, the agents "attempted to gather more information by doing a 'knock and talk' interview with the hope of being able to conduct a consent search."[108]

On the morning of August 27, 2004, two federal agents and one local police detective arrived at the Andrus residence.[109] One of the federal agents was a "forensic computer expert . . . [who] waited outside in his car for . . . authorization to enter the premises."[110] Dr. Bailey Andrus—a ninety-one-year-old retired physician—greeted the agents at the door and invited them inside.[111] Once inside, the agents "learned that Ray Andrus lived in the center bedroom in the residence . . . [and] did not pay rent and lived in the home to help care for his aging parents."[112]

The federal agent "testified he could see the door to Ray Andrus'[s] bedroom was open and asked Dr. Andrus whether he had access to the bedroom."[113] Dr. Andrus informed agents that he did have access and "felt free to enter the room when the door was open, but always knocked if the door was closed."[114]

After the agents obtained written consent from Dr. Andrus to search any computers inside the house, the computer forensic specialist was brought inside to conduct a forensic search of Ray Andrus's computer.[115] The court described the process as follows:

> Kanatzar [the computer analyst] removed the cover from Andrus'[s] computer and hooked his laptop and other equipment to it. Dr. Andrus testified he was present at the beginning of the search but left the bedroom shortly thereafter. Kanatzar testified it took about ten to

105. United States v. Andrus, 483 F.3d 711, 713 (10th Cir. 2007), *petition for cert. filed*, No. 07-0753 (U.S. Nov. 21, 2007).
106. *Id.*
107. *Id.*
108. *Id.*
109. *Id.*
110. *Id.*
111. *Id.*
112. *Id.*
113. *Id.*
114. *Id.*
115. *Id.*

> fifteen minutes to connect his equipment before he started analyzing the computer. Kanatzar used EnCase forensic software to examine the . . . hard drive. *The software allowed him direct access to the hard drive without first determining whether a user name or password were needed.* He, therefore, did not determine whether the computer was protected by a user name or password prior to previewing the computer's contents.[116]

While still at the house Kanatzar identified "depictions of child pornography" on Andrus's computer.[117]

Meanwhile, the other federal agent learned from Dr. Andrus that the only computer in the house was the one in Ray Andrus's room.[118] At this point, the court notes that there was conflicting testimony during the trial. Either the father or the federal agent suggested that Ray Andrus be contacted about the search at his place of employment.[119] Regardless, the father made the call and then handed the phone to the agent to speak with Andrus.[120] After Andrus agreed to come home, the federal agent went into the bedroom and asked Kanatzar to stop the computer search.[121] Next, "Kanatzar testified he shut down his laptop computer and waited in Ray Andrus'[s] bedroom with the computer until [the other federal agent] came back into the room to tell [Kanatzar] Andrus had personally consented to the search and Kanatzar could continue."[122]

When Andrus arrived home a few minutes later, the federal agent informed him "that officers had already been inside the residence and had looked through his room."[123] After explaining that he obtained Andrus's father's consent to search the computer, the federal agent "verbally asked Andrus for consent to search his room and his computer."[124] Andrus agreed and the agents then resumed the search.[125]

Andrus was subsequently indicted for possession of child pornography.[126] Andrus filed a motion to suppress the evidence on grounds that it

---

116. *Id.* at 713-14 (emphasis added). The court added in a footnote that "Kanatzar testified that someone without forensic equipment would need Ray Andrus'[s] user name and password to access files stored within Andrus'[s] user profile." *Id.* at 714 n.1.

117. *Id.* at 714.

118. *Id.*

119. *Id.*

120. *Id.* There was also conflicting testimony about the content of this phone call. The federal agent testified that he did not inform Andrus of the nature of the search, but Andrus testified that the agent "told him during the phone call that pornography had been discovered during a search of his computer." *Id.* at 714 n.3. However, the court noted that because the consent search ultimately rested upon apparent authority, there was no need to resolve this dispute. *Id.* Accordingly, because the voluntariness of Andrus's consent to search his computer was not the basis for the consent search, it does not matter what the agent said to him during the phone conversation. *See id.*

121. *Id.* at 714.

122. *Id.*

123. *Id.*

124. *Id.*

125. *Id.*

126. *Id.* at 712.

was obtained in violation of the Fourth Amendment.[127] Specifically, Andrus argued that his father did not voluntarily consent to the search; that his father "lacked actual authority to consent to a search of the computer, even if he had authority to consent to a search of [his] room"; and that his father "could not reasonably be seen as having authority to consent to a search of the computer and, thus, lacked apparent authority."[128]

The court concluded that the father did voluntarily consent, but that the father did not have actual authority for the computer search.[129] The court reasoned that the father "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."[130] However, the court concluded that the father did possess apparent authority, reasoning that "the agents' belief that [the father] had authority to consent to a search of the computer was reasonable up until the time they learned there was only one computer in the house."[131] Further, because Kanatzar was instructed to "suspend the search at that point, there was no Fourth Amendment violation."[132] Consequently, because the motion to suppress was denied Andrus pled guilty and was sentenced to seven months in prison.[133]

B. The Tenth Circuit Affirms Andrus's Conviction

1. Majority Opinion

Writing for a 2-1 majority, Judge Murphy began the discussion of *Andrus* by reviewing cases dealing with consent searches and the Fourth Amendment.[134] Specifically, he identified and discussed the cases addressing third party consent searches.[135] After reviewing several relevant cases, Judge Murphy noted that "[t]his court has not previously considered expectations of privacy associated with a home computer in a third party consent situation."[136] Moreover, "Tenth Circuit precedent thus far has dealt only with computer searches where police have a warrant or

127. *Id.* at 715.
128. *Id.*
129. *Id.*
130. *Id.*
131. *Id.* The court based its conclusion that the father had apparent authority on five factual findings: (1) the e-mail address used to register for the website was in the father's name; (2) the father told the agents that he paid the bill for the Internet access; (3) the agents were aware that several other people lived in the household; (4) Ray Andrus's bedroom was unlocked, suggesting that the members of the household had access to it; and (5) "the computer itself was in plain view of anyone who entered the room and it appeared available for anyone's use." *Id.*
132. *Id.*
133. *Id.* at 712.
134. *Id.* at 716.
135. *Id.*
136. *Id.* at 717.

other justification for searching the computer, or when the defendant computer owner himself has consented to the search."[137]

Next, Judge Murphy addressed the issue of whether computers are like other containers, or if they are something entirely different.[138] The majority acknowledged that "[g]iven the pervasiveness of computers in American homes, this court must reach some, at least tentative, conclusion about the category into which personal computers fall."[139] Subsequently, the majority reasoned that because computers play such a central role in multiple areas of our lives, "it seems natural that computers should fall into the same category as suitcases, footlockers, or other personal items that command . . . a high degree of privacy."[140]

The court then addressed the issue of whether one has a reasonable expectation of privacy by having a password-protected computer file.[141] In an analysis regarding containers such as footlockers or suitcases, the key inquiry is whether the "container is physically locked."[142] However, the court quickly recognized the challenge in identifying whether a container is locked and whether a computer—which has been categorized by the court as a container—is also locked. Essentially, one can visibly see a lock on containers, but how is one to tell if a computer is locked, "especially when the computer is in the 'off' position prior to the search[?]"[143] The court determined that "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."[144] So, whether a person has a reasonable expectation of privacy in a password-protected computer file depends primarily on whether the police have any reason to suspect the person's password is needed to access the computer.

Finally, the court addressed the "critical issue [of] whether, under the totality of the circumstances known to [the agents], these [agents] could reasonably have believed Dr. Andrus [had] authority to consent to a search of the computer."[145] Emphasizing that "[i]f the circumstances reasonably indicated Dr. Andrus had mutual use of or control over the computer, the officers were under no obligation to ask clarifying ques-

137. *Id.* (The cases Judge Murphy cited are: United States v. Brooks, 427 F.3d 1246 (10th Cir. 2005); United States v. Tucker, 305 F.3d 1193 (10th Cir. 2002); and United States v. Carey, 172 F.3d 1268 (10th Cir. 1999)).
138. *Id.* at 718.
139. *Id.*
140. *Id.*
141. *Id.*
142. *Id.*
143. *Id.*
144. *Id.* at 719.
145. *Id.* at 720.

tions . . . ."[146] Hence, there is no burden on the police to confirm what they already reasonably believe. This is true "even if . . . the burden would have been minimal in this particular case."[147] Consequently, the majority concluded that it was reasonable to believe that Dr. Andrus had apparent authority, thus holding that the subsequent search of Andrus's computer was not a violation of the Fourth Amendment.[148]

2. Judge McKay's Dissent

Judge McKay was concerned with "the majority's implicit holding that law enforcement may use software deliberately designed to automatically bypass computer password protection based on third-party consent *without the need to make a reasonable inquiry* regarding the presence of password protection and the third party's access to that password."[149] He suggested that the majority's holding would allow police to maneuver around the Fourth Amendment with regard to passwords. Invoking the reasoning of Chief Justice Roberts's dissent in *Georgia v. Randolph*—another third party consent case—Judge McKay suggested that the majority holding in *Andrus* denied a computer owner the ability to manifest an expectation of privacy by utilizing a password.[150] Specifically, "[t]he unconstrained ability of law enforcement to use forensic software . . . to bypass password protection without first determining whether such passwords [exist] does not exacerbate this difficulty . . . rather, it avoids it altogether, simultaneously and dangerously sidestepping the Fourth Amendment in the process."[151] Under the majority rule, having a password is a meaningless protection unless the user makes it clear that there actually is a password requirement to access the computer.

Judge McKay also noted that even though password protection is not immediately visible, this "does not render it unlocked."[152] So, because law enforcement agents cannot see a lock, that does not mean that it is not there, and, furthermore, this reality only heightens the need for inquiry about the presence of a lock.

Judge McKay reasoned that "[g]iven the inexcusable confusion in this case, the circumstantial evidence is simply not enough to justify the agents' use of . . . software without making further inquiry [regarding the

146. *Id.*
147. *Id.* (responding to the dissent's charge that the police should carry some burden to resolve any ambiguities about actual authority).
148. *Id.* at 722.
149. *Id.* (McKay, J., dissenting) (emphasis added).
150. *Id.* at 723 (McKay, J., dissenting).
151. *Id.*
152. *Id.*

presence of a password]."[153] In order to remedy this situation, Judge McKay recommended that—given relevant case law on consent searches and computer searches—the law should require government agents to "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."[154]

3. Andrus's Petition for Rehearing

The Tenth Circuit subsequently denied Andrus's request for rehearing.[155] The court noted in its order denying rehearing that "its opinion is limited to the narrow question of the apparent authority of a homeowner to consent to a search of a computer . . . in the specific factual setting presented . . . ."[156] Further, the court did not address "the extent of capability and activation of password protection . . . on home computers . . . or the degree to which law enforcement confronts password protection . . . on home computers."[157] Although *Andrus* presented key questions about issues of privacy and passwords, the court did not offer an explicit opinion about how to confront these issues.

III. ANALYSIS

A. Other Circuit Court Opinions

Andrus was a case of first impression for the Tenth Circuit.[158] There were only two other appellate court cases identified involving third party consent of a password-protected computer and both were heard by the Fourth Circuit.[159] *Trulock v. Freeh*[160] involved a couple living together and sharing a computer, but they each had password-protected files to which the other did not have access.[161] A key factual distinction between *Freeh* and *Andrus* was that in *Freeh*, the "agents queried [the girlfriend] about [appellant's] personal records and computer files" and

153. *Id.* at 725 (McKay, J., dissenting) (adding that the agents were clearly aware of the uncertainty of the father's authority to consent when they stopped the search to wait for Andrus to arrive home).

154. *Id.*

155. United States v. Andrus, 499 F.3d 1162, 1162 (10th Cir. 2007) (opinion denying rehearing) (reporting that eight judges voted to deny rehearing and five judges voted to grant rehearing).

156. *Id.* (opinion denying rehearing).

157. *Id.* at 1163 (opinion denying rehearing).

158. United States v. Andrus, 483 F.3d 711, 717 (10th Cir. 2007), *petition for cert. filed*, No. 07-0753 (U.S. Nov. 21, 2007) (stating that "[t]his court has not previously considered expectations of privacy associated with a home computer in a third-party consent situation. Tenth Circuit precedent thus far has dealt only with computer searches where police have a warrant . . . or when the defendant computer owner himself has consented to the search.").

159. There are a few more cases involving third-party consent of a *non*-password protected computer. *See, e.g.*, United States v. Aaron, 33 F. App'x 180, 182 (6th Cir. 2002); United States v. Smith, 27 F. Supp. 2d 1111, 1113 (C.D. Ill. 1998).

160. 275 F.3d 391 (4th Cir. 2001).

161. *Id.* at 403.

were told that there was a password.[162] Reasoning that "because he concealed his password from [his girlfriend], it cannot be said that [he] assumed the risk that [she] would permit others to search his files," the Fourth Circuit concluded that third party consent was valid as to a general search of the computer but did not extend to the password-protected files.[163]

The Fourth Circuit emphasized that the presence of a password conveyed that the appellant had "affirmatively intended to exclude . . . others from his personal files."[164] Hence, the appellant had a reasonable expectation of privacy that narrowed the scope of the third party consent.[165] Importantly, however, *Freeh* appeared to suggest that it is not unreasonable for law enforcement to enquire about the presence of a password in the course of obtaining third party consent to search a computer.

In *United States v. Buckner*,[166] government agents obtained consent from the appellant's wife to search his password-protected computer for evidence of online fraud.[167] The Fourth Circuit held the apparent authority of the wife was reasonable and thus held the search valid.[168] *Buckner* addressed the issue of the use of technology that bypasses passwords because the agents were never informed about the presence of a password.[169] Further, "[e]ven during the . . . forensic analysis processes, nothing the officers saw indicated that any computer files were encrypted or password-protected."[170] Echoing *Kyllo*, the court added in a footnote that "[w]e do not hold that the officers could rely upon apparent authority to search while simultaneously using . . . technology to intentionally avoid discovery of [a password] put in place by the user."[171] Interestingly, this is precisely what government agents did in *Andrus*.[172]

B. The Relevance of Kyllo

Andrus's defense was an attack on the court's holding that his father had authority to consent to the search.[173] Andrus challenged the reasonableness of the agent's reliance on information provided by his father

162. *Id.* at 398.
163. *Id.* at 403.
164. *Id.*
165. *Id.*
166. 473 F.3d 551 (4th Cir. 2007).
167. *Id.* at 552.
168. *Id.*
169. *Id.* at 553.
170. *Id.* at 555.
171. *Id.* at 556 n.3.
172. There is no evidence that the agents in *Andrus* used the technology to intentionally avoid having to ask about the presence of a password. United States v. Andrus, 483 F.3d 711, 723 (10th Cir. 2007), *petition for cert. filed*, No. 07-0753 (U.S. Nov. 21, 2007). However, because the software itself is capable of deliberate avoidance of a password, it is reasonable to conclude that this eliminates the need to ask about the presence of a password.
173. *Id.* at 712.

and argued that the court erroneously concluded it was reasonable to believe that his father had authority to consent.[174] At trial, however, Andrus did not challenge the use of specialized technology that bypasses password-protection on computers.[175] Consequently, Andrus missed an opportunity to let *Kyllo* do the heavy lifting of his defense.

In order to support this assertion, Andrus would have needed to lay the following groundwork. First, courts—including the Tenth Circuit in *Andrus*—have held that computers are like containers for purposes of search and seizure rules.[176] Second, courts have consistently held that locked containers carry a higher expectation of privacy, and thus the scope of a third party consent search is limited.[177] These two premises lead to the critical question: is a password like a lock?

1. The *Andrus* Court Held That a Computer is Like a Container.

The court recognized that computers have similarities and differences from traditional containers.[178] After all, containers are used to place personal items in for storage and safe-keeping and transporting from place to place. When computers first appeared they were largely viewed as "glorified typewriters" which could hardly be compared to a container.[179] But over time computers have gradually become the central storage space for large swaths of individuals' personal lives. Consequently, the court concluded that "[b]ecause intimate information is commonly stored on computers, it seems natural that computers should fall into the same category as suitcases, footlockers, or other personal items that command a high degree of privacy."[180]

2. The Presence of a Lock on a Container Receives More Fourth Amendment Protection.

When government agents opened up a locked footlocker—without a search warrant and without consent—the Court held that "by placing personal effects inside a double-locked footlocker, respondents manifested an expectation [of privacy.] No less than one who locks the doors of his home against intruders, one who safeguards his personal possessions [with a lock] is due the protection of the Fourth Amendment Warrant Clause."[181] The Tenth Circuit followed this by observing that the

174. *Id.* at 715.

175. United States v. Andrus, 499 F.3d 1162, 1163 (10th Cir. 2007) (opinion denying rehearing) (reasoning that "appellant's argument premised on *Kyllo v. United States* . . . was made for the first time in his petition for rehearing and was not initially presented to the panel. The argument is therefore forfeited.").

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

177. United States v. Chadwick, 433 U.S. 1, 11 (1977); United States v. Block, 590 F.2d 535, 541 (4th Cir. 1978).

178. *Id.* at 718.

179. Kerr, *supra* note 60, at 569.

180. *Andrus*, 483 F.3d at 718 (internal quotation) (empty brackets omitted).

181. *Chadwick*, 433 U.S. at 11.

presence of a lock on a container is a factor in determining the expectation of privacy.[182] The Fourth Circuit has also held that when a mother did not have a key, her third party consent did not extend to her son's locked footlocker.[183]

Conversely, the absence of a lock carries with it an inference that the owner does not have a reasonable expectation of privacy, thus broadening the scope of the consent of a third-party to authorize a search. The salient point is that a locked container triggers increased protections under the Fourth Amendment. If something is locked, and the only key is in the hands of the owner, courts require more than third party consent for the search to be valid.[184]

3. The Critical Question: Is a Password on a Computer Like a Lock on a Container?

If Andrus could convince the court that a password is like a lock, then the argument would be over because the syllogism would be complete. All locked containers get more protection; all password-protected computers are like locked containers; therefore, all password-protected computers get more protection.

The court made the following statements on the issue of whether a password is like a lock: "Determining whether a computer is locked . . . presents a challenge distinct from that associated with other types of closed containers"; and "[u]nlike footlockers or suitcases . . . a *lock* on the data within a computer is not apparent from a visual inspection . . . of the computer . . ."; and "[d]ata on an entire computer may be protected by a password, with the password functioning as a *lock* . . . ."[185] The court also quoted from a dictionary definition of "password" which described it as "[a] sequence of characters, known only to authorized persons, which must be keyed in to gain access to a particular computer . . . ."[186]

After reading these comments, it appeared that the court was about to announce that a password was like a lock and hold that unless Andrus's father had the password, the search of the computer was invalid. However, the court reasoned that because the password was not immediately visible to the agents, and because the agents were under no obligation to ask about the presence of a password—absent ambiguities suggesting the need for further inquiry—then, as a matter of law, there

182. United States v. Salinas-Cano, 959 F.2d 861, 864 (10th Cir. 1992).
183. United States v. Block, 590 F.2d 535, 537, 542 (4th Cir. 1978).
184. *Id.*
185. *Andrus*, 483 F.3d at 718-19 (10th Cir. 2007) (emphasis added) (internal quotation omitted).
186. *Id.* at 719 (quoting Oxford English Dictionary Online, http:// dictionary. oed.com (entry for "Password," definition 1.b).

was no password.[187] In other words, the test of whether a password on a computer is like a lock is not whether the password actually operates as a lock, but whether "law enforcement knows or should reasonably suspect because of surrounding circumstances that the computer is password protected."[188] So, even though Andrus locked his computer—thus exhibiting an increased expectation of privacy that carries with it increased protections—the court reasoned that his computer was not locked because there was no way for the agents to know that it was locked. This holding, combined with the holding that the father had apparent authority, provided the Tenth Circuit with the support it needed to affirm the conviction.

4. Could *Kyllo* Have Helped Andrus?

Kyllo could have helped *Andrus* because "where . . . the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[189] Similarly, in *Andrus*, "the Government use[d] a device [called EnCase software] that is not in general public use, to explore details of [Andrus's computer] that would previously have been unknowable without" turning on the computer, entering the password and accessing the files.[190]

Imagine a person has locked their personal container—like a footlocker—by using a magnetized locking device not immediately visible to others.[191] Also, the device is unlocked by waving a demagnetizing wand over it that only the owner has access to. If law enforcement agents get valid third party consent to search the container, they are accordingly armed with the authority to try to open it and search its contents. However, upon realizing they cannot open it because it is locked by the unseen magnet, and because only the owner has the demagnetizing wand, the third party consent to search the container evaporates. Unless the third party consenter also has a demagnetizing wand that will open the container, the third party consent is rendered toothless and the agents will be unable to search the container without a warrant or consent of the owner. Simply put, the presence of a lock—seen or unseen—that effectively keeps the agents out is supported by the Constitution.

Now, in the same scenario, would it be reasonable for agents to use an imaging device that identifies the contents of the container without

187. *Id.* at 721.
188. *Id.* at 719.
189. Kyllo v. United States, 533 U.S. 27, 40 (2001).
190. *Id.*
191. These types of mechanisms are becoming more common on doors and the magnets are turned on and off to control access in the same way deadbolts are used. The obvious difference being that deadbolts are visible whereas magnets are not.

first trying to open it? Put another way, if agents had a tool like x-ray machine, would it be reasonable for them to use this tool on the container without ever having to open the container, thus rendering the presence of a lock irrelevant? According to the United States Supreme Court, the answer is no.[192] *Kyllo* stands for the proposition that the government cannot use certain special technologies to gather information in areas protected by the Fourth Amendment without a search warrant.[193] Thus, it is reasonable to conclude that a *Kyllo*-based argument could have changed the Tenth Circuit's decision in *Andrus*.

It is possible that *Andrus* stands for the proposition that the use of *Kyllo*-like technology is constitutional when there is third party consent. However, this would be inconsistent with the Supreme Court's Fourth Amendment jurisprudence. Consider that if it were Andrus's locked footlocker agents wanted to search for images of child pornography, the agents would have had to have the father's apparent authority *and* a key. Now, if *Andrus* is allowed to stand, all agents need to search a container is third party apparent authority and *something less* than a key.

The *Andrus* rule essentially does three things: first, it removes the requirement for a third party consenter to have a key to a locked container; second, it replaces the key requirement with a government actor's reasonable belief that there is no need for a key; and third, it allows the use of technology to bypass a key (or password) without first determining whether the container (or computer) is locked. This new rule will likely result in increased litigation over Fourth Amendment protections because of the unfettered discretion given to law enforcement agents in searches of private containers, including computers.

It is hard to imagine what private citizens could reasonably do to protect themselves against excessive government intrusion into their private lives when all that is required is for a police officer to *not* suspect the presence of a lock and to possess the technology to bypass it. One of these tools without the other is limited and within the scope of the Fourth Amendment in certain contexts. But the combination conveys formidable powers to the government and delivers a significant blow to any reasonable expectations of privacy a citizen might have over private information.

---

192. *Id.* at 40.

193. Specifically, *Kyllo* limits the technology to that "not in general public use." *Id.* Thus, Andrus would have had to convince the Tenth Circuit that EnCase software is not in general public use. Further, the use of the technology in *Kyllo* was on a house, not a computer. However, given that the computer was located in a bedroom inside the house, it seems reasonable to infer that the Court would view this as an area protected by the Fourth Amendment.

CONCLUSION

It is clear that the digital age has ushered in new challenges for the courts. What remains unclear, however, is the approach that will properly balance the tension between individual freedoms and valid state interests in an unprecedented time of technological development.

The Tenth Circuit's approach in *Andrus* appears to narrow individual protections in favor of broader state authority to search for private information. But is this an accurate reading of *Andrus* in light of the context? While this case comment presents an argument that *could* have won for Andrus, it may be important to briefly ask whether Andrus *should* have won. In fairness to the Tenth Circuit, the narrowing of individual freedoms appears to be the national trend as the government seeks to balance freedom and security. Further, as criminal activity becomes more sophisticated through the use of computer technology, it is reasonable to conclude that government agents charged with fighting computer crime should be given some latitude and discretion in how to confront these complicated matters.

The *Andrus* court, however, went a step beyond what is reasonably necessary to combat computer crimes. There were alternative methods available to government agents—such as getting a search warrant or asking about the presence of a password. Also, because of the increasingly central role that computers play in the storage of personal information, courts should be less deferential to government attempts to access that information without search warrants.

Consequently, courts will—and should—face increased scrutiny as they review critical matters involving the scope and authority of government agents to investigate crimes in the digital age.

Michael Smith[*]

---

* J.D. Candidate, 2009, University of Denver Sturm College of Law. The author would like to thank Professor Sam Kamin and Melissa Meitus for guidance and support with this comment, as well as Shannon Brown, Brad Brickhouse, Kelly Wilson, and the *Denver University Law Review* board and staff for their editing assistance.