Cleveland State Law Review

Volume 57 | Issue 2 Note

2009

Dangerously Sidestepping the Fourth Amendment: How Courts Are Allowing Third-Party Consent to Bypass Warrants for Searching Password-Protected Computer

David D. Thomas

DANGEROUSLY SIDESTEPPING THE FOURTH AMENDMENT: HOW COURTS ARE ALLOWING THIRD-PARTY CONSENT TO BYPASS WARRANTS FOR SEARCHING PASSWORD-PROTECTED COMPUTERS

DAVID D. THOMAS*

*J.D. expected, May 2010, Cleveland State University, Cleveland-Marshall College of Law; M.B.A. University of Findlay; B.B.A. Tiffin University. The Author would like to thank Alexis Osburn, Prof. Janice Aitken, and Prof. Karen Mika for their input and guidance.

I. INTRODUCTION

Imagine laboring away at work all day, only to receive a phone call from your elderly parent who tells you that police officers have arrived at your home and are making a copy of your personal computer's password-protected hard drive—without a warrant. This is exactly what happened to 52-year-old Ray Andrus.[1] Without a doubt, any judge would suppress evidence collected in such a manner, right? Wrong. The court in *United States v. Andrus*[2] refused to suppress the seized evidence, holding that Ray Andrus's 91-year-old father had "apparent authority" over a password-protected private computer located in Ray's personal bedroom.[3]

The Fourth Amendment to the U.S. Constitution[4] sets the ultimate regulation as to how the government can conduct searches and seizures.[5] Specifically, it states that "no Warrants shall issue, but upon probable cause . . . and particularly describing the place to be searched, and the persons or things to be seized."[6] Over time, courts have carved out many exceptions to the warrant requirement.[7] One of those is the exception allowing a third party to give consent to a warrantless search or seizure when that party has some interest or control over the property being searched or seized.[8] Even without bringing into account the complexities of technology and password-protected data, dealing with this exception by itself has been a thorn in the side of many courts.[9] Then throw into the mix not only personal computers, but also their ability to house voluminous amounts of data that can be, and often is, password-protected. In terms of personal computers and warrantless searches of them, how much latitude do third parties have in authorizing law enforcement to search a computer that is owned by someone else, but is located in the same household? The *Andrus* case is among the first to attempt to tackle the

---

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

[2] *Id.*

[3] *Id.* at 722.

[4] U.S. CONST. amend. IV.

[5] *Id.* The Fourth Amendment in totality reads:

> 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.

Id.

[6] *Id.*

[7] The Fourth Amendment: Search and Seizure Law, http://www.house.leg.state.mn.us/hrd/pubs//ss/clss4th.htm 9 (last visited Mar. 9, 2009). Among those exceptions are the plain view doctrine, the automobile exception, and exigent, or emergency, circumstances. *Id.* This Note focuses on "third-party consent," an extension of the consent exception. The consent exception allows a law enforcement officer to conduct a warrantless search or seizure when he or she reasonably believes a party has the authority to consent to such activity. *Id.*

[8] 18 AM. JUR. 2D *Proof of Facts* § 681 (2008).

[9] *Id.*

issue and shows how courts are having a difficult time dealing with third-party consent to search computers.[10]

One thing is certain: The courts are willing to admit that passwords on computers are synonymous with physical locks on physical containers, but are struggling to apply Fourth Amendment protections to warrantless third-party consent searches of password-protected computers. This Note will look at not only the third-party consent exception to the Fourth Amendment, but also more specifically, the legal issues raised when that exception is used to admit evidence from a warrantless search of a password-protected computer. At issue are two differing viewpoints of how to deal with computers: whether the computer is simply a physical box that can be looked at to view the contents, or whether passwords on the computer liken it to a "locked box" that protects the virtual contents.[11] Technological advances can allow law enforcement to use forensic software and devices to access computer data without regard to any password "locks" that may be activated on the computer.[12] In the *Andrus* dissent, Judge Monroe G. McKay wrote that "the unconstrained ability of law enforcement to . . . bypass password protection without first determining whether such passwords have been enabled . . . dangerously sidestep[s] the Fourth Amendment."[13]

In totality, this Note sets forth that it is unacceptable for law enforcement to ignore the presence of passwords simply because they may not be immediately visible. Furthermore, it is contrary to the Fourth Amendment for law enforcement to rely on third parties who grant access to search the data without knowledge of the password to unlock the data. Principles hammered out over time for searches and seizures of physically locked objects[14] can easily be transposed and extended to fit the virtual world while still providing people the protections of the Fourth Amendment.

This Note examines how Fourth Amendment protections are being sidestepped because of the problems raised in dealing with passwords on personal computers as locks, specifically when a third party consents to a warrantless search of a computer. Part II of this Note will look at the background of the Fourth Amendment and the third-party consent exception. Part III provides a basic understanding of how computer hard drives, operating systems, and forensic software function. Part IV

---

[10]Pamela A. MacLean, *Courts Grapple With Computer Searches: Is It a Password Protected 'Locked Box' or a Simple Container?*, NAT'L L.J., May 15, 2007, available at http://www.law.com/jsp/article.jsp?id=1179092588804.

[11]*Id.*

[12]*Andrus*, 483 F.3d at 713-14.

[13]*Id.* at 723. Judge McKay took issue with the 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." *Id.* at 722.

[14]If a third party does not have a key to a locked item, police cannot reasonably rely on third-party consent. *See, e.g.*, United States v. Block, 590 F.2d 535, 537 (4th Cir. 1978) (holding that although a mother had the authority to allow a search of her house, she did not have such authority over her son's footlocker when she had no key to open it and it was "fastened shut by some means that indicated to the officers that it was locked and that a key was required to open it").

looks at the reasonable expectation of privacy test[15] adopted by the Supreme Court and how it has been applied to certain types of technology. Part V analyzes the application of third-party consent to locked containers and to computers in general. Part VI dissects the application of these principles in the only three cases[16] to specifically deal with passwords as locks when a third-party has consented to a warrantless search of a computer. Finally, Part VII offers a reasonable, common-sense approach to password-protected computers based on a foundation of principles hammered out over time for other locked containers.

II. THE FOURTH AMENDMENT AS A FOUNDATION FOR PRIVACY

During the drafting of the Constitution, a man from Virginia by the name of George Mason called for a Bill of Rights to be included.[17] He and others like him believed that the primary purpose of government was to protect peoples' rights.[18] These included the freedoms of speech and religion,[19] the right to bear arms,[20] and the right to be secure from unlawful searches and seizures.[21] While the Bill of Rights was ratified in 1791,[22] it would be fifteen years before a case involving search and seizure would come before the Supreme Court.[23] Nevertheless, it was abundantly clear from the framers of the amendment that it is the right of all American citizens "to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures."[24]

A. The Fourth Amendment

The principles of the rights guaranteed in the Fourth Amendment predate the Constitution itself. In colonial America, British officers would make sweeping searches of homes and businesses using general writs of assistance to ensure no

---

[15]*See infra* Part II.A.

[16]*See infra* Part VI.

[17]CHARLES M. WETTERER, THE FOURTH AMENDMENT: SEARCH AND SEIZURE 18 (1998).

[18]*Id.* While George Mason wanted the Bill of Rights included into the Constitution, another delegate, Roger Sherman, spoke out against it. *Id.* at 18-19. Explaining that the many state constitutions already provided for certain rights, he was able to convince enough others to vote against it. *Id.* at 18. When the Constitution was completed, Mason refused to sign it because it did not contain a Bill of Rights. *Id.* at 19.

[19]U.S. CONST. amend. I.

[20]U.S. CONST. amend. II.

[21]U.S. CONST. amend. IV.

[22]WETTERER, *supra* note 17, at 22.

[23]*Id.* at 24. In 1806, a merchant by the name of John Buford provoked his customers to such an extent that they complained to fourteen justices of the peace. *Id.* The justices issued a warrant for his arrest on the grounds that he was not of a good name and that horrible grievances such as murder could arise. *Id.* at 24-25. When Buford could not post a bond of $4,000 to assure his good behavior, he was jailed. *Id.* at 25. The Supreme Court ordered him released because the warrant stated no offense. *Id.*

[24]U.S. CONST. amend. IV.

goods were being smuggled in from countries other than England.[25] These general writs of assistance could be used repeatedly and required no oath or level of specificity of what was to be searched.[26] One of the more well-espoused cases from England, *Entick v. Carrington*,[27] involved state officers using general warrants to raid homes searching for materials that attacked the government and the King. Entick sued because the officers had gone through all of his personal belongings, drawers, and papers, including locked desks and boxes.[28] The court stated that to make such a practice legal "would be subversive of all the comforts of society."[29] The court also declared that probable cause and specificity of what was to be searched or seized is required in the issuing of a warrant.[30]

Although people in England enjoyed a higher level of privacy,[31] no protection from these writs existed for colonial America until the British were overthrown.[32] John Adams said, on the eve of the American Revolution, "an Englishmen's dwelling House is his Castle. The law has erected a Fortification around it."[33] The language of the Fourth Amendment encapsulates the mantra that "a person's home is his castle."[34] This fundamental principle can only be superseded by law enforcement when they have reason to believe a crime has taken place and the search they wish to conduct is narrowly tailored to find the specified evidence.[35] In a factual situation giving rise to a Fourth Amendment claim, the Supreme Court has stated that the "capacity to claim the protection of the Amendment depends not upon a property right in the invaded place but upon whether the area was one in which there was a

---

[25]MICHAEL ROGERS RUBIN, PRIVATE RIGHTS, PUBLIC WRONGS: THE COMPUTER AND PERSONAL PRIVACY 9 (1988).

[26]*Id.*

[27]Entick v. Carrington, (1765) 95 Eng. Rep. 807 (K.B.).

[28]*Id.*

[29]*Id.* at 817.

[30]*Id.* at 812. The court stated that when issuing a warrant for stolen goods, that "it is never granted, but upon the strongest evidence that a felony has been committed, and that the goods are secreted in such a house; and it is to seize such goods as were stolen, not all the goods in the house." *Id.*

[31]William Pitt, an eighteenth century British statesman perhaps said it best when in a speech before Parliament he declared:

> The poorest man may in his cottage bid defiance to all the forces of the Crown. It may be frail, its roof may shake, the wind may blow through it, the storm may enter, the rain may enter, but the King of England cannot enter! All his force dares not cross the threshold of the ruined tenement!
>
> United States v. Ross, 456 U.S. 798, 822 n.1 (1982) (quoting William Pitt).

[32]RUBIN, *supra* note 25, at 10.

[33]HARRY HENDERSON, PRIVACY IN THE INFORMATION AGE 14 (1999).

[34]*See* U.S. CONST. amend. IV.

[35]HENDERSON, *supra* note 33, at 15.

reasonable expectation of freedom from governmental intrusion."[36] The modern standard by which courts consider whether a search has occurred is a two-pronged test from Justice Harlan's concurring opinion in *Katz v. United States*.[37] In making that determination, an analysis looks at whether (1) a person has a subjective expectation of privacy, and (2) "the expectation [is] one that society is prepared to recognize as reasonable."[38]

B. The Third-Party Consent Exception and Apparent Authority

Courts have devised exceptions to the Fourth Amendment's warrant requirement over the course of history.[39] One well-recognized exception occurs when a party gives law enforcement consent to conduct a warrantless search.[40] Most relevant to this discussion of the consent exception is when a third party, who is not the primary target of the search, grants that consent. Generally, when a person has some interest in the property in question, that person may grant consent to a search that is in fact directed at a different person.[41] Although the Supreme Court has held third-party consent searches valid,[42] the guidelines courts use to navigate through this type of consent are "vague and general."[43]

---

[36]Mancusi v. DeForte, 392 U.S. 364, 368 (1968). In fact, a year earlier, in *Warden v. Hayden*, the Court said:

> The premise that property interests control the right of the Government to search and seize has been discredited. Searches and seizures may be 'unreasonable' within the Fourth Amendment even though the Government asserts a superior property interest at common law. We have recognized that the principal object of the Fourth Amendment is the protection of privacy rather than property, and have increasingly discarded fictional and procedural barriers rested on property concepts.

387 U.S. 294, 304 (1967). One Justice rationalized that property interest is not the proper analysis, and concluded that if it were, "then much of our daily lives will be unshielded from unreasonable governmental prying, and the reach of the Fourth Amendment will have been narrowed to protect chiefly those with possessory interests in real or personal property." Rakas v. Illinois, 439 U.S. 128, 166 (1978) (White, J., dissenting).

[37]389 U.S. 347 (1967).

[38]*Id.* at 361 (Harlan, J., concurring). Justice Harlan explained his analysis of the two prong test,

> [t]hus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.

Id.

[39]*See, e.g.*, sources cited *supra* note 7.

[40]18 AM. JUR. 2D *Proof of Facts* § 681 (2008).

[41]John B. Wefing & John G. Miles, Jr., *Consent Searches and the Fourth Amendment: Voluntariness and Third Party Problems*, 5 SETON HALL L. REV. 211, 211-12 (1973).

[42]*See* United States v. Matlock, 415 U.S. 164, 171 (1974).

[43]18 AM. JUR. 2D *Proof of Facts* § 681 (2008).

[44]*Id.* Early cases used an "agency approach" that took into account an implied agency relationship between the person who consented and the suspect of the search. *Id.* This theory

Several theories have evolved over time to help understand the validity of third-party consent to searches.[44] The theory that has gained large acceptance in third-party warrantless consents is the "possession and control" rule.[45] This theory focuses on the third party's independent right to consent to the search and takes into account the third party's relationship to the property that is being searched.[46] The prosecution "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."[47] A variation of the possession and control test, the "apparent authority" test, looks at the apparent authority of the consenter to give that consent.[48] Here, the consent is held valid when law enforcement reasonably believes that the consenter had authority over the place or object in question.[49] However, the Supreme Court has made it clear that "the rights protected by the Fourth Amendment are not to be eroded by strained applications of the law . . . or by unrealistic doctrines of 'apparent authority.'"[50]

Courts have thus needed to decide at what point common authority is had over a given premises or property so that the third party has the right to consent to the search. Generally, if a consenter has equal or superior rights of use and access, then that third party can grant consent.[51] However, inferior rights of a third-party consenter cannot give rise to a valid consent.[52] A cornucopia of factors are used to determine common authority over property, including monetary relationships, familial relationships, actual possession, and de facto control.[53] The Supreme Court has held that the law of property does not apply when determining the justification of

---

held that the third party was an agent of the suspect and thus had the ability to consent to the search. *Id.* A second approach is called the "status relationship" approach, which looks at the consenter's mere relationship to the suspect (e.g. husband/wife) to determine if the consent is valid. *Id.* Both of these approaches have been largely rejected. *Id.*

[45] *Id.*

[46] *Id.*

[47] *Matlock*, 415 U.S. at 171.

[48] 18 AM. JUR. 2D *Proof of Facts* § 681 (2008).

[49] *Id.*

[50] Stoner v. California, 376 U.S. 483, 488 (1964). The Court went on to explain:

> [I]t is unnecessary and ill-advised to import into the law surrounding the constitutional right to be free from unreasonable searches and seizures subtle distinctions, developed and refined by the common law in evolving the body of private property law which, more than almost any other branch of law, has been shaped by distinctions whose validity is largely historical. We ought not to bow to them in the fair administration of the criminal law. To do so would not comport with our justly proud claim of the procedural protections accorded to those charged with crime.

Id.

[51] Georgia v. Randolph, 547 U.S. 103, 106 (2006).

[52] 18 AM. JUR. 2D *Proof of Facts* § 681 (2008).

[53] Wefing & Miles, *supra* note 41, at 262.

third-party consent.[54] Rather, the authority rests on "mutual use of the property by persons generally having joint access or control for most purposes."[55]

When the apparent authority doctrine is used, the searching officer's reasonable belief of the third-party consenter's authority is taken into account.[56] Under the apparent authority doctrine, a third party can consent to a search if a police officer reasonably, but erroneously, believes that the third party has the actual authority to consent.[57] The objective inquiry looks at whether the facts available to the officer at the moment allow a reasonable person to believe that the third party had authority over the premises.[58] However, if an officer is faced with an ambiguous situation with respect to the authority of a third party to consent, he cannot disregard that ambiguity.[59] Rather, he has a duty to ask questions and make a further investigation prior to relying on the consent.[60]

III. COMPUTER CONCEPTS AND SOFTWARE FORENSIC BASICS

There can be no doubt that technology plays a pivotal role in the daily lives of people everywhere. Even back in 1982, *Time* magazine changed its annual "Man of the Year" to "Machine of the Year."[61] A writer of that issue commented, "computers were once regarded as distant, ominous abstractions, like Big Brother. In 1982, they truly became personalized, brought down to scale, so that people could hold, prod and play with them."[62] Since then, computer crime has also caught on. It has become so prevalent, that the Department of Justice maintains a website specifically for reporting on computer crimes.[63] While such crimes are what eventually lead us to a discussion on warrantless searches of computers based on third-party consent, it

---

[54]*See* sources cited *supra*, note 36.

[55]*Matlock*, 415 U.S. at 172 n.7.

[56]18 AM. JUR. 2D *Proof of Facts* § 681 (2008).

[57]Illinois v. Rodriguez, 497 U.S. 177, 186 (1990).

[58]United States v. Kimoana, 383 F.3d 1215, 1222 (10th Cir. 2004). The court in this case further went on to explain that "the burden [of proving effectiveness of consent] cannot be met if agents, faced with an ambiguous situation, nevertheless proceed without making further inquiry." *Id.* Furthermore, "[w]arrantless entry is unlawful without further inquiry if circumstances make it unclear whether the property about to be searched is subject to mutual use by the person giving consent." *Id.*

[59]*Id.*

[60]*Id.*

[61]Computer History Museum, http://www.computerhistory.org/timeline/?category=ppc (last visited Mar. 19, 2009). Interestingly enough, the main writer wrote his article on a typewriter, and would not upgrade for another year. *Id.*

[62]*Id.*

[63]United States Department of Justice: Computer Crime and Intellectual Property Section, http://www.cybercrime.gov/ccips.html (last visited Mar. 19, 2009). This department of the government is responsible for implementing strategies to combat computer and intellectual property crimes. *Id.* The department "prevents, investigates, and prosecutes computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts." *Id.*

is helpful to understand some fundamentals of how computers and forensic software operate.

A. Hard Drives and Operating Systems

Several articles discussing searches and seizures have gone into great depths on the technological aspects of how data is stored on computer hard drives, how the technology works when individuals access data on a hard drive, and how forensic software interacts with files on hard drives.[64] While a detailed understanding is not necessary for this Note, a brief overview of the technology will help provide a foundation for understanding the conflict courts face in viewing computers as a physical box or a virtual one for purposes of searches and seizures.

When law enforcement searches a computer for evidence, the primary location of data storage being searched is the hard drive.[65] A hard drive within a computer is made up of many interconnected mechanical and electrical parts sealed in a container.[66] The main part inside that container is a series of round discs, or platters, stacked on top of one another.[67] Data is stored on the surface of each platter.[68] Each

---

[64]*See generally* Ty E. Howard, *Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files*, 19 BERKELEY TECH. L.J. 1227 (2004) (discussing data on a hard drive, specifically with respect to Internet browsing); Lloyd S. van Oosternrijk, Comment, *Paper or Plastic?: Electronic Discovery and Spoliation in the Digital Age*, 42 HOUS. L. REV. 1163 (2005) (discussing how data gets stored and erased on a hard drive); Wayne Jekot, *Computer Forensics, Search Strategies, and the Particularity Requirement*, 7 U. PITT. J. TECH. L. & POL'Y 2 (2007) (discussing computer forensics).

[65]Hard Disk Home, http://www.harddiskhome.com (last visited Mar. 19, 2009). Specifically,

> [i]n any computer system the hard disk is considered as the secondary memory device that is used for the primary data storage. The primary memory is obviously the RAM. But as the RAM is the primary memory it cannot be used for the purpose of the permanent data storage. Hence a secondary memory device is necessarily needed for the purpose of the data storage in any computer system. Apart from hard disk drive the tape storage media can also be used as the secondary storage device. But the hard disk drive is the most popularly used secondary memory device. The main reason for this is the access speed and the reliability of the data it can offer. In the case of the tape drives the access speed is much lower and the data transfer is comparatively low than the hard disk drive.

Id.

[66]PC Guide: Hard Disk Operational Overview, http://www.pcguide.com/ref/hdd/op/over.htm (last visited Mar. 19, 2009). Round, flat disks known as platters that are coated with a special material to store data in the form of magnetic patterns. *Id.* These platters are then stacked on top of one another on a spindle. *Id.* A motor spins the platters at a very high speed. *Id.* Devices that are able to read the magnetic patters, called heads, are mounted onto sliders and use electromagnetic charges to either read data from the disk or record information to it. *Id.* The sliders are attached to arms and are connected and positioned over the surface of the disk. *Id.* A device known as a logic board works with the rest of the computer and helps to control the components. *Id.*

[67]PC Guide: Hard Disk Platters and Media, http://www.pcguide.com/ref/hdd/op/media.htm (last visited Feb. 10, 2008). Specifically,

> [e]very hard disk contains one or more flat disks that are used to actually hold the data in the drive. These disks are called platters . . . They are composed of two main

platter contains concentric circles called tracks and each concentric circle is further divided into smaller sections called sectors.[69] While data is stored on these sectors, they are too small for modern operating systems, such as Microsoft Windows, to work with.[70] The operating system groups these sectors together into units called clusters.[71] It is then the operating systems job to manage the data.[72]

The operating system is the computer's master control program.[73] Its job is to act as the interface between the hardware and the individual, including the software the individual uses.[74] The operating system provides a user interface,[75] job management,[76] task management,[77] device management,[78] data management,[79] and security.[80] In terms of data management, the operating system keeps track of where data is physically stored on each sector of a hard drive.[81] Whenever an individual wishes to save or delete data from the hard drive, he or she must instruct the operating system to interact with the hard drive to complete the request.[82]

---

substances: a *substrate* material that forms the bulk of the platter and gives it structure and rigidity, and a *magnetic media coating* which actually holds the magnetic impulses that represent the data. Hard disks get their name from the rigidity of the platters used, as compared to floppy disks and other media which use flexible "platters."

Id.

[68]*Id.*

[69]Marshall Brain, *How Hard Disks Work*, http://computer.howstuffworks.com/hard-disk7.htm (last visited Mar. 19, 2009).

[70]Hard Drive Clusters and File Allocation, http://www.dewassoc.com/kbase/hard_drives/clusters.htm (last visited Mar. 19, 2009).

[71]*See* Brain, *supra* note 69.

[72]TechEncyclopedia, http://www.techweb.com/encyclopedia/defineterm.jhtml?term=OPERATINGSYSTEM (last visited Mar. 19, 2009).

[73]*Id.*

[74]*Id.*

[75]A user interface includes the graphical menus and windows that help the computer user and the computer interact. *Id.*

[76]Job management refers to the scheduling of the order in which programs are run. *Id.*

[77]Task management is the ability to perform more than one task at a time—multitasking. *Id.*

[78]Device management involves the controlling of all other hardware associated with the machine and sending that hardware commands to work for the user. *Id.*

[79]Data management is the process of keeping track of where data is stored, whether on a hard drive, an optical disk, or tape, or any other type of media. *Id.*

[80]Security can include password protection, activity logs, and accounting of time. *Id.*

[81]*Id.*

[82]*Id.*

One of the major features of the security aspect of an operating system is that of password protection. Password protection is designed to specifically keep unauthorized users from accessing data.[83] It allows a single user of a computer to keep others out and allows multiple users of a single machine to have their own secure accounts.[84] While there are several types of operating systems available today, including MacOS and Linux, over eighty-eight percent of computers run the Microsoft Windows operating system.[85] Windows XP and Windows Vista allow for separate user accounts and passwords, known as profiles.[86] Each user is able to set personal preferences, and the operating system blocks each user from accessing another user's profile and data.[87] Password-protected user accounts allow for an expectation of privacy that others without the password will not gain access to private information. It is through this aspect of a computer where the issue arises whether to treat a computer as a "locked box" that protects the virtual contents, as opposed to a physical box for open viewing.[88]

B. Forensic Software

Password protection is also relevant for purposes of forensic analysis of hard drives. Forensic analysis of hard drives has the ability to bypass passwords completely, thus making passwords irrelevant.[89] In a nutshell, "computer forensics is the analysis of information contained within and created with computer systems and computing devices, typically in the interest of figuring out what happened, when it happened, how it happened, and who was involved."[90] One of the more widely used

---

[83]Strong Passwords: How to Create and Use Them, http://www.microsoft.com/protect/yourself/password/create.mspx (last visited Mar. 19, 2009).

[84]Windows Vista Help: What is a User Account, http://windowshelp.microsoft.com/Windows/en-US/Help/5d82b9b6-0a55-4199-b5d1-5b25b6b106cb1033.mspx (last visited Mar. 12, 2009).

[85]Operating System Market Share, http://marketshare.hitslink.com/report.aspx?qprid=8 (last visited Mar. 4, 2009). Coming in second place is the Macintosh operating system at approximately ten percent and the Linux operating system is third at under one percent. *Id.*

[86]User Account Control Overview, http://technet.microsoft.com/en-us/windowsvista/aa906021.aspx (last visited Feb. 10, 2008).

[87]Create and Customize User Accounts, http://www.microsoft.com/windowsxp/using/setup/winxp/accounts.mspx (last visited Mar. 4, 2009).

[88]MacLean, *supra* note 10.

[89]Steve Thompson, *How Computer Forensic Investigators (CFIs) Recover Evidence*, ASSOCIATED CONTENT, Jan. 4, 2008, *available at* http://www.associatedcontent.com/article/487557/how_computer_forensic_investigators.html.

[90]Steve Hailey, *What is Computer Forensics?*, http://www.cybersecurityinstitute.biz/forensics.htm (Sept. 19, 2003). Computer forensics can be used to analyze and determine the root cause of a system failure or why a system is not operating in the manner for which it is designed. *Id.* In addition, computer forensics can be used to figure out who has been misusing a computer system and to what extent that misuse has occurred. *Id.* Computer forensics helps law enforcement determine if a crime has been committed on a computer or against a computer system. *Id.* Also, "[i]n many cases, information is gathered during a computer forensics investigation that is not typically available or viewable by the average

forensic software tools is EnCase by Guidance Software.[91] Forensic software such as this allows law enforcement to make an identical copy of a hard drive without regard to the presence of any operating system on the hard drive.[92] The forensic software creates a "bitstream" copy of the hard drive that includes all sectors, whether they have data on them or not.[93] In addition, this includes data that may have been previously deleted by an individual.[94] This is because when an individual "deletes" data from a hard drive, the operating system only marks the sectors as empty so that they can be written to again.[95] However, the original data is still there until the user "saves" another file onto that sector.[96] Even though the data may appear gone to the operating system, forensic software allows law enforcement to retrieve that data.[97] Because the forensic investigator is not turning on the computer in the normal sense, there is no operating system and are no passwords with which to be bothered. Investigators work with hard drives on a physical level where every file is capable of being searched and opened. In this scenario, operating system features, such as password protection, are not a concern. It is through this very fundamental makeup of a computer where the issue arises whether to treat a computer as a physical box or as a "locked box" that protects the virtual contents.[98]

IV. SEARCHING, SEIZING, AND TECHNOLOGY

While the Fourth Amendment may have originally been intended to be very specific, applying only to intrusions by the federal government,[99] its scope has been

---

computer user, such as deleted files and fragments of data that can be found in the space allocated for existing files." *Id.*

[91]Guidance Software, http://www.guidancesoftware.com (last visited Mar. 4, 2009).

[92]How EnCase Forensics Works, http://www.guidancesoftware.com/products/ef_works.aspx (last visited Mar. 4, 2009).

[93]Basics of Computer Forensics, http://www.cybercontrols.net/forensics/attorneyforensicbasics.asp (last visited Mar. 4, 2009). A bitstream copy is:

> "the technical term for the end-product of a forensics acquisition of a computer's hard drive. . . . The bit-stream copy involves the copying of every bit of data on an 'evidence' hard drive, which includes the file slack, and unallocated file space in which 'deleted' files and e-mails are frequently recovered from."

Id.

[94]*Id.* To explain, "a . . . common assumption by computer users when . . . delet[ing] a document . . . on . . . [a] computer is that that file is forever gone. This could not be further from the truth. In fact, the deleted file has been re-assigned to the slack space of the hard drive." *Id.* Furthermore, while a computer user cannot see the deleted file, "a bit-stream copy and subsequent examination of the slack space will likely reveal the contents of the entire document." *Id.*

[95]Howstuffworks, http://computer.howstuffworks.com/question578.htm (last visited Mar. 4, 2009).

[96]*Id.*

[97]Hailey, *supra* note 90.

[98]MacLean, *supra* note 10.

[99]Wolf v. Colorado, 338 U.S. 25 (1949).

greatly extended since its ratification.[100] Societal changes and population increases resulted in a higher number of government searches.[101] Government searches were most prevalent for a long time in investigations of violations of liquor prohibition laws and sales and use of drugs.[102] However, advancements in technology led to more questions on the use of government searches.[103] Telephone communications, professional cameras, aerial surveillance, the Internet, and computer records all add on to the complexities of analyzing suspected governmental violations of the Fourth Amendment.[104] When Supreme Court members change, often the interpretation of the Fourth Amendment does as well.[105] What constitutes a legal search still remains unclear to many people up to this day—even judges.[106]

A. The Rule for Expectations of Privacy

As of 2003, almost sixty-two percent of all U.S. households had a computer.[107] In addition to changing the way people go about their daily business, computers have also changed how crimes are committed.[108] It has become necessary for courts to examine how the Fourth Amendment applies to law enforcement's searches and seizures of computer data. While this Note looks at warrantless searches and seizures, a completely different analysis has been conducted on what types of data law enforcement officers can search for on a computer once they have a warrant and are sifting through the contents of a computer hard drive.[109] These include questions about what law enforcement should be restricted to when searching a hard drive, whether it be by file names, file types, or certain keywords.[110] Whether new

---

[100]WETTERER, *supra* note 17, at 89.

[101]*Id.* at 90.

[102]*Id.*

[103]*Id.*

[104]*Id.*

[105]*Id.* at 91.

[106]*Id.* The Supreme Court has issued around 400 opinions that involve the Fourth Amendment, a great many of which have been by five-to-four decisions. *Id.*

[107]Households with Computers, 1998 and 2003, http://www.infoplease.com/ipa/A0931441.html (last visited Mar. 4, 2009).

[108]David. J. S. Ziff, *Fourth Amendment Limitations on the Execution of Computer Searches Conducted Pursuant to a Warrant*, 105 COLUM. L. REV. 841, 841 (2005).

[109]*Id.* at 845-52. In one case, after lawfully seizing a computer, the officers obtained a warrant to search the computer for "names, telephone numbers, ledger receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances." *Id.* at 846. The detective, after browsing through the files, came across images of child pornography. This posed a problem for the court as to what evidence should be allowed. The court ultimately allowed in all the evidence concerning controlled substances, up to and including the first child pornography picture opened. *Id.* at 848. However, the court suppressed all pictures opened afterwards as not being part of the warrant's requirements. *Id.*

[110]Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L.J. 193, 205-10 (2005). One argument states

technology is seen as a means of endless possibilities or as being out of control with negative effects on identity and privacy, its integration into daily life is met with tense regulation.[111]

Computers are not the first technological advancements that have caused problems for the courts. In 1928 in *Olmsted v. United States*,[112] the Supreme Court held that the tapping of a person's phone line from outside his or her house was acceptable.[113] The Court stated that protection from the Fourth Amendment came only through protection from physical intrusions.[114] This resulted in Presidents giving the FBI expanded authority to wiretap and increased the usage of electronic surveillance.[115] It was not until 1967 in *Katz v. United States*[116] that the Court would overturn the requirement of physical intrusion and declare that "what 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."[117]

Justice Harlan's concurrence in *Katz* brought forth the "reasonable expectation of privacy" test, the test employed today in determining whether Fourth Amendment protections have been violated.[118] This is a two-pronged test that looks at whether (1) a person has a subjective expectation of privacy, and (2) "the expectation [is] one that society is prepared to recognize as reasonable."[119] Due to privacy concerns that stem from the use of computers, Fourth Amendment analysis in terms of the

---

that law enforcement should not be restrained by certain file types, such as ".jpg" for a picture. *Id.* at 207-08. The reasoning is that most people who want to hide something will "intentionally mislabel files, or attempt to bury incriminating files within innocuously named directories." *Id.* at 209 (quoting United States v. Gray, 78 F. Supp. 2d 524 (E.D. Va. 1999)). Therefore, law enforcement need not "accept as accurate any file name or suffix and limit [the] search accordingly." *Id.*

[111]HENDERSON, *supra* note 33, at 13. Henderson opines, "How do people decide how to respond to the challenge of a technology that is as ripe with unforeseeable consequence as the invention of writing itself?" *Id.* He states that one way is through regulation, and that "the telephone, the automobile, TV—all have been integrated into society through a combination of regulation and social custom." *Id.*

[112]277 U.S. 438, 466 (1928), *overruled by* Katz v. United States, 389 U.S. 347, *and* Berger v. New York, 388 U.S. 41.

[113]*Id.*

[114]*Id.*

[115]Daniel J. Solove, The Digital Person: Technology and Privacy in the Information Age 199 (2004).

[116]389 U.S. 347 (1967).

[117]*Id.* at 351 (citations omitted).

[118]SOLOVE, *supra* note 115, at 198. Solove notes that change over time "brings into existence new conditions and purposes. Subtler and more far-reaching means of invading privacy have become available to the government." *Id.* (quoting Olmstead v. United States, 277 U.S. 438, 473 (1928) (Brandeis, J., dissenting)). Thanks to technological changes, it is "possible for the government, by means far more effective than stretching on the rack, to obtain disclosure in the court of what is whispered in the closet." *Id.*

[119]SOLOVE, *supra* note 115, at 198 (quoting *Katz*, 380 U.S. at 361 (Harlan, J., concurring)).

searching and seizing of computers and the data contained on them "must be approached cautiously and narrowly."[120]

B. Applying the Rule to Technology

After the Supreme Court announced the reasonable expectation of privacy test in *Katz*, the Court had the opportunity to address the reasonableness of certain technologies in searches, including aerial surveillance and thermal imaging. In *Florida v. Riley*,[121] the defendant had a partially covered greenhouse in his backyard.[122] A police officer observed the interior of that greenhouse while circling 400 feet above in a helicopter.[123] While the defendant met the first prong of the test by taking precautions to prevent observation from the ground,[124] the Court held that he could not reasonably expect privacy from a helicopter flying above the greenhouse because the helicopter was flying within the bounds of the law.[125] In *Kyllo v. United States*,[126] law enforcement aimed a thermal imaging device at a home from a public street to detect relative amounts of heat within the home.[127] The Court held that a search has occurred when the "Government uses a device that is not in general public use, to explore the details of the home that would previously have

---

[120]People v. Gall, 30 P.3d 145, 165 (Colo. 2001) (Martinez, J., dissenting). This must be done "because of the important privacy concerns inherent in the nature of computers, and because the technology in this area is rapidly growing and changing." *Id.*

[121]488 U.S. 445 (1989).

[122]*Id.* at 448.

[123]*Id.*

[124]*Id.* at 450. The Court recognized that "[t]wo sides of the greenhouse were enclosed. The other two sides were . . . obscured from view. . . . The greenhouse was covered by corrugated roofing panels . . . [and a] wire fence surrounded the mobile home and the greenhouse, and the property was posted with a 'DO NOT ENTER' sign." *Id.* at 448.

[125]*Id.* at 450-52. The Court took careful notice to indicate that not all aircraft activity by law enforcement could be lawful, and that flying a few feet below legal airspace or kicking up some dust might be enough for a different analysis:

> This is not to say that an inspection of the curtilage of a house from an aircraft will always pass muster under the Fourth Amendment simply because the plane is within the navigable airspace specified by law. But it is of obvious importance that the helicopter in this case was *not* violating the law, and there is nothing in the record or before us to suggest that helicopters flying at 400 feet are sufficiently rare in this country to lend substance to respondent's claim that he reasonably anticipated that his greenhouse would not be subject to observation from that altitude. Neither is there any intimation here that the helicopter interfered with respondent's normal use of the greenhouse or of other parts of the curtilage. As far as this record reveals, no intimate details connected with the use of the home or curtilage were observed, and there was no undue noise, and no wind, dust, or threat of injury.

Id.

[126]533 U.S. 27 (2001).

[127]*Id.* at 29-30.

been unknowable without physical intrusion . . . and is presumptively unreasonable without a warrant."[128]

In many cases, such as *Andrus*, law enforcement use forensic devices and software to access data on a computer's hard drive.[129] These forensic tools allow law enforcement to ignore the existence of password locks and to search through data on a hard drive.[130] While the use of this technology may be appropriate in certain situations, such as when a legal warrant has been obtained, its use on password-protected computers when authorized by third parties presents troubling results from a Fourth Amendment privacy perspective.[131]

V. ANALYZING WARRANTLESS THIRD-PARTY CONSENT SEARCHES

The vast majority of computer searches take place under the auspices of a warrant.[132] As such, dealing with warrantless third-party consents to password-protected computer searches has not been an easy task for appellate courts to deal with.[133] In fact, only three circuit courts have touched on this specific situation.[134] Before discussing those three cases, however, an analysis of what courts have held to be the standard for searching locked containers,[135] as well as what the courts have done with computers in general, is necessary.

A. When There Is No Key to a Locked Container, There Is No Third-Party Consent

Even when police have been given consent to search an area by a third party under the rubric of apparent authority, that consent has been held to not apply to locked or otherwise protected areas where the party giving authority does not have the "key" to the locked area.[136] This principle has tested true time and time again.[137]

---

[128] *Id.* at 40.

[129] United States v. Andrus, 483 F.3d 711, 713-14 (10th Cir. 2007).

[130] *Id.*

[131] *Id.* at 723 (McKay, J., dissenting) (explaining that "[t]he fact remains that [forensic software's] ability to bypass security measures is well known to law enforcement).

[132] *Id.* at 722 n.1.

[133] *See* MacLean, *supra* note 10.

[134] *Id.*

[135] It has been long established that "[c]ontainers are a well-defined category within Fourth Amendment law." Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 550 (2005). In fact, "[t]he foundational premise of the container cases is that opening a container constitutes a search of its contents; if a person has a reasonable expectation of privacy in the contents of a container, opening the container and seeing the contents violates that reasonable expectation of privacy." *Id.*

[136] *See, e.g.*, United States v. Bell, 357 F. Supp. 2d 1065 (N.D. Ill. 2005); State v. Harris, 642 A.2d 1242 (Del. 1993); People v. Snipe, 841 N.Y.S.2d 763 (N.Y. Sup. Ct. 2007).

[137] To name just a few cases illustrative of this, in State v. Harris, 642 A.2d 1242 (Del. 1993), the court found that a mother could consent to a search of her son's room, but not a locked toolbox. *Id.* at 1248. Furthermore, it was unreasonable for the police to assume authority when they knew it was locked, and the mother did not have the key. *Id.* at 1248-49. In *State v. Smith*, 966 S.W.2d 1 (Mo. Ct. App. 1997), the court held the defendant's girlfriend

In *United States v. Block*,[138] police serving an arrest warrant were conducting a general search of a home. Mrs. Block, the homeowner, consented to the search of her 23-year-old son's room.[139] Inside the room, officers found a padlocked footlocker belonging to the son.[140] Mrs. Block did not possess a key to the footlocker.[141] The officers forced open the footlocker and found heroin.[142] In determining that the authority to search the room did not extend to the locked footlocker, the court relied on the son's expectations of privacy.[143] When a particular object is secured or is generally known for preserving privacy, it is unreasonable to confront such a secure container and force it open when the third party has no shared access to the container.[144] The fact that the legal-aged son was a mere occupant of the home allows for a finding that he assumed the risk that his mother could allow a general search of the house and even his room.[145] However, that assumption of the risk does not expand, in such circumstances, to every discreet enclosed space.[146]

---

did not have apparent authority to consent to a search of a locked safe. *Id.* at 8. The officers pried open the safe with a hammer, crowbar, and screwdriver. *Id.* There was no evidence that the girlfriend had any interest in the safe or its contents. *Id.* at 8-9. In *People v. Snipe*, 841 N.Y.S.2d 763 (N.Y. Sup. Ct. 2007), the court held that a mother had no authority to consent to a search of a closet when the defendant placed a lock on it and did not provide a key to the mother. *Id.* at 770-772.

[138]590 F.2d 535 (4th Cir. 1978).

[139]*Id.* at 537. Police were serving an arrest warrant for an individual who was known to reside at Mrs. Block's house. *Id.* The police and Mrs. Block provided differing views of how the consent was given. *Id.* The police testified that prior to forcing open the locked trunk, they obtained a signed consent form to search her son's room and take anything that could be used as evidence. *Id.* Mrs. Block claimed that she received the consent form only after the police opened the trunk and seized the items. *Id.* She claimed the police described the form to her as a receipt for the items that were seized. *Id.*

[140]*Id.* at 537.

[141]*Id.*

[142]*Id.* at 538.

[143]*Id.* at 541.

[144]*Id.* at 541. In a footnote, the court chastised the police for acting in such a manner when it said, "Here, all the circumstances presented to the police indicated the wisdom, as well as the relative convenience of seeking a search warrant to inspect the footlocker's interior." *Id.* at 541 n.9.

[145]*Id.* at 541.

[146]*Id.* at 541. The court acknowledged that "common experience[s] of life" are to be considered in "assessing the existence and the reasonableness of privacy expectations." *Id.* Furthermore, "it surely teaches all of us that the law's 'enclosed spaces' mankind's valises, suitcases, footlockers, strong boxes, etc. are frequently the objects of his highest privacy expectations" and that expectations of privacy are "at their most intense . . . when such effects are kept semi-permanently in public places or in places under the general control of another." *Id.*

This principle of protection is essential to the "primary objects of people's ordinary expectations of privacy."[147]

The particular item to be searched need not even be secured with a lock in the typical sense. It is enough that the item in question is one that is personal to someone and is not mutually used by the third person giving consent. In *Marganet v. State*,[148] the defendant's girlfriend consented to a search of their hotel room.[149] The police ultimately found illegal drugs inside the defendant's shaving kit, which was located inside his suitcase.[150] Acknowledging that the girlfriend retained actual authority over the hotel room,[151] the court held that she lacked authority to consent to the search of the shaving kit and the suitcase.[152] The court determined that the items searched were personal to the defendant, were closed and sitting up against a wall, and were inappropriately searched when the third party was unsure of the contents and gave no indication that she had permission to access them or mutually used them.[153] These facts could not lead officers to a reasonable belief of apparent authority over the items without further inquiry.[154] Even in cases where the container is not locked, it is imperative that an officer take steps to obtain sufficient facts on which to base a decision as to whether the third party has "common authority over the . . . property to be searched."[155]

From these illustrative examples, the rules of third-party consent, and the limitations thereof, are well-solidified. When individuals live together, they assume the risk that one of the individuals may consent to searches of common areas of a home and shared objects.[156] When an object is locked and the third-party individual does not have a key to the lock, it is unreasonable for law enforcement to believe

---

[147]*Id.* The court indicated that in cases like this it is hard to imagine how the "manifestations of retained expectations of privacy by the absent person could be stronger, or the indications of assumed risks of third person permission to inspect, lower." *Id.*

[148]927 So. 2d 52 (Fla. 2006).

[149]*Id.* at 53.

[150]*Id.*

[151]*Id.* at 56.

[152]*Id.* at 61.

[153]*Id.* The court explained, after reviewing a number of relevant cases, that a number of factors come into play when determining the rights of a third party to consent to a search. *Id.* at 56-60. Factors included are "whether the property clearly belongs to one person, whether it is generally used by one person, whether it is freely accessible to others, whether the container is closed or open, whether it is locked or unlocked, and whether orders have been given not to open the container." *Id.* at 60.

[154]*Id.* In drawing a distinction, the court said that "it is less reasonable for a police officer to believe that a third party has full access to a defendant's purse or a briefcase than, say, an open crate." *Id.*

[155]*Id.* at 61. Possession of a container does not imply automatic authority to consent to a search. The court stated that "[f]or purposes of searches of closed containers, mere possession of the container by a third party does not necessarily give rise to a reasonable belief that the third party has authority to consent to a search of its contents." *Id.* at 61.

[156]*See* sources cited *supra*, note 137.

there is shared access to the object, and they cannot rely on the third person's authority to grant consent to a search.[157] Furthermore, when law enforcement is faced with an ambiguous situation as to whether the third party has authority to consent to a search, it is imperative that they take appropriate steps and ask appropriate questions to make a determination.[158] Willful blindness is not an option.

B. Analyzing Warrantless Searches of Computers

These principles of an expectation of privacy have not been wholly lost when applied to data stored on computers in general. When individuals place data in files on the hard drive of their computers, they manifest a reasonable expectation of privacy in the contents of those files.[159] In fact, a heightened expectation of privacy can be said to exist, at least when it comes to files that have been deleted. One court has held that deleted files are not analogous to trash put out on the treelawn.[160] While there may be no expectation of privacy in the trash that one throws out,[161] when it comes to forensic recovery of deleted files under Fourth Amendment analysis, an individual does not abandon the right to privacy of computer files by virtue of deleting them.[162]

Courts have also previously addressed the warrantless searching of a computer in a handful of factual scenarios that involve third-party consent and computers in general. An analysis of these cases helps to understand the state of affairs before addressing the main issue of password-protected computers and third-party consent. For instance, even when a computer hard drive is delivered to another person for repairs, the reasonable expectation of privacy of the data on the hard drive is not forgone. In *United States v. Barth*,[163] the defendant provided his hard drive to a technician who was also an FBI confidential informant.[164] When the technician found child pornography, he was instructed to make a copy of the hard drive.[165] Law enforcement subsequently searched the hard drive.[166] Likening the hard drive to a locked container, the court held the expectation of privacy was in the contents of the

---

[157] *Id.*

[158] *See supra*, note 147.

[159] People v. Carratu, 194 Misc. 2d 595, 603 (N.Y. Sup. Ct. 2003).

[160] United States v. Upham, 168 F.3d 532 (1st Cir. 1999). The court rejected the reasoning that "by deleting the images, [the defendant] 'abandoned' them and surrendered his right of privacy. Analogy is a hallowed tool of legal reasoning; but to compare deletion to putting one's trash on the street where it can be searched by every passer-by . . . is to reason by false analogy." *Id.* at 537 n.3.

[161] *See* California v. Greenwood, 486 U.S. 35, 43 (1988).

[162] *See supra* note 159.

[163] 26 F. Supp. 2d 929 (W.D. Tex. 1998).

[164] *Id.* at 932.

[165] *Id.*

[166] *Id.* at 933.

container, not the container itself.[167] Therefore, when the technician charged with the sole task of fixing the hard drive allowed police to search it, the police conducted a warrantless search in violation of the Fourth Amendment.[168] In this case, the technician did not have "joint access" to the hard drive for most purposes and the police could not have reasonably believed that he had the apparent authority to consent to the search.[169]

Yet another scenario constituting a violation of the Fourth Amendment involving consent turned on a lack of authority even though the consenter was the lessee of the premises and owned some of the computer equipment in question. In *United States v. Durham*,[170] a case involving counterfeit currency, the defendant lived in an unattached garage next to his mother's house that had been converted into a bedroom.[171] Law enforcement suspected that computer equipment, some of which the mother owned, was being used to create counterfeit currency.[172] The mother consented to a search, but had no keys that worked on any of the doors.[173] Police subsequently pried open a window to gain entrance.[174] The mother had been completely denied access to the room, had never been in the room alone, and had never used the computer equipment.[175] The court concluded that the police failed to make a reasonable inquiry as to the authority the mother had over the room and the computer.[176] Failure to make a reasonable inquiry as to the extent of the authority is unjustifiable.[177]

---

[167] *Id.* at 936-37. The court explained that "the Fourth Amendment protection of closed computer files and hard drives is similar to the protection it affords a person's closed containers and closed personal effects." *Id.* Furthermore, "a warrant is usually required to search the contents of a closed container, because the owner's expectation of privacy relates to the contents of that container rather than to the container itself. *Id.* And that "[b]y placing data in files in a storage device such as his hard drive, . . . [the] Defendant manifested a reasonable expectation of privacy in the contents of those files. These files should therefore be afforded the full protection of the warrant requirement." *Id.*

[168] *Id.* at 937.

[169] *Id.* at 938. The court stated that, "it is clear that [the technician] did not have actual authority to consent to a search of Defendant's hard drive. [The technician] was in possession of the unit for the limited purpose of repair." *Id.* Furthermore, it was unreasonable for law enforcement to believe that the technician had the authority. *Id.* They knew he was a technician and an FBI informant and only possessed the hard drive in a limited capacity. *Id.*

[170] No. 98-10051-02, 1998 U.S. Dist. LEXIS 15482 (D. Kan. Sept. 11, 1998).

[171] *Id.* at *2.

[172] *Id.* at *3.

[173] *Id.* The defendant's mother actually handed over three keys to the police officers, but none of them worked to gain entrance to the garage room. *Id.*

[174] *Id.* at *4. The court explained, "When the officers were unable to enter the bedroom using one of her keys, they tried to enter through the windows which would not open manually. The officers finally entered the room by prying open a screen window and crawling inside." *Id.*

[175] *Id.* at *10-11.

[176] *Id.* at *11-12. Here, "the officer knew that the defendant had physically excluded his mother from the bedroom. He deliberately chose not to ask questions which should have

This is not to say that courts have not swung the other way on occasion and found there to be no violation of the Fourth Amendment when it comes to computers in general. In *Walsh v. State*,[178] a case involving child molestation, the defendant's wife consented to a warrantless search of a computer located in their home.[179] The computer had been purchased by the wife and was available to the entire family, including their children.[180] While nothing in the record indicated the existence or use of password protection, the defendant nevertheless objected to the search on the grounds the history of his Internet browsing on the computer were private in that they were his "personal thoughts and associations."[181] The court disagreed with the defendant.[182] Co-inhabitants of a household assume the risk that any of the other co-inhabitants can authorize a search of a common area.[183] Where a computer is generally open and available to the entire family in a common area, any member of the family may authorize a search of that computer.[184]

In another instance involving the upholding of the constitutionality of a search of a computer, the defendant's girlfriend phoned police to make a search of the computer where she suspected child pornography.[185] In this case, the computer was in an open area, was not password-protected, and was used by others in the defendant's absence.[186] Other facts supporting the constitutionality of the search include the fact that the live-in girlfriend maintained joint access of the bedroom area where the computer was located and that the defendant attempted to teach the girlfriend how to use the computer.[187] The facts here show that officers could reasonably believe that the third party authorizing consent had apparent authority to do so.[188] Of particular importance in this case is the emphasis the court places on the computer as having no password protection.[189] While there is no discussion as to

---

immediately occurred to any officer attempting to determine in good faith whether Mrs. Durham had the authority to consent to enter the room." *Id.*

[177] *Id.* at *12.

[178] 512 S.E. 2d 408 (Ga. Ct. App. 1999).

[179] *Id.* at 411.

[180] *Id.*

[181] *Id.*

[182] *Id.*

[183] *Id.* at 412.

[184] *Id.* The court stated that "[u]nder these circumstances, [the defendant's] wife had the authority to consent to the seizure of the computer, because she had common authority over the premises as well as over the computer itself." *Id.*

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

[186] *Id.* at 1114.

[187] *Id.*

[188] *Id.* at 1116.

[189] In several places, the court references the lack of password protection on the machine. "Mr. Gasparin testified that the computer was not password protected." *Id.* at 1114. "Ms.

whether there would have been a different outcome if password protection were present, the court stated that "it is important to note that none of the officers who searched the computer found passwords on the computer," and that "this belies [d]efendant's claim of exclusive and possessory control."[190] The lack of passwords on the computer played a pivotal role in the outcome of the case.

A third party's apparent authority over a computer does not strip the primary user of that computer of Fourth Amendment rights simply by virtue of the object in question being a computer. If the computer is in a common area of the living space and is generally used by the third party, then there is a lesser expectation of privacy and it is more reasonable for law enforcement to believe that the third party can indeed consent to a search.[191] A lack of the presence of a password also demonstrates a lower expectation of privacy.[192] However, when the computer has been placed in a separate area where the third party has no or limited access, it is less reasonable for law enforcement to assume a third party's apparent authority to consent to a search.[193] In any instance, it is still for law enforcement to take reasonable, minimal steps, such as asking questions, to determine whether the third party's consent is valid before conducting a warrantless search.[194]

VI. MAKING A MESS OUT OF COMPUTER SEARCHES, PRIVACY, AND THIRD-PARTY CONSENT

As previously mentioned, only three cases have come before courts dealing with third-party consent to search computers that were password-protected or otherwise contained a mechanism for privacy. The issues of password protection and what information law enforcement should know about the computer in question created a troubling outcome in each of the three cases.

A. The First Two Circuit Decisions Lay the "Groundwork"?

In *United States v. Morgan*,[195] a wife suspected her husband of viewing child pornography. After the spy software that she installed indicated as much, she contacted local law enforcement.[196] Although the wife had her own computer and never used the one in question, it was located in a common area of the house where

---

Denise Walls, sister of Defendant, testified that if the officers were allowed access to DOS immediately, then the password protection must have been deactivated." *Id.* "Defendant testified that . . . he had removed the passwords . . . [and] admitted that certain graphics files could have been viewed without the need for passwords. *Id.* "Neither Mr. Gasparin nor the FBI examiner who later examined the computer found any passwords on the computer system." *Id.*

[190] *Id.* at 1116.

[191] *See supra* notes 177-83 and accompanying text.

[192] *See supra* notes 188-89 and accompanying text.

[193] *See supra* notes 169-74 and accompanying text.

[194] *See supra* note 176 and accompanying text.

[195] 435 F.3d 660 (6th Cir. 2006).

[196] *Id.* at 662.

the wife had access—the basement.[197] And although the computer had no password protection, the husband had installed software designed to erase Internet content.[198] Regardless of the fact that she never used the computer and had her own computer elsewhere in the house,[199] a fact she neglected to tell police prior to the search, the court relied on the apparent authority of the wife over the computer in upholding the constitutionality of the search.[200] While the results of this case may be easier to swallow than the results of the *Andrus* case discussed below, it still raises unanswered questions of what constitutes privacy with respect to computers and exactly what information officers have to know prior to conducting a warrantless search.

In *United States v. Buckner*,[201] an online fraud investigation led police to a home without a warrant with the intent to seize a computer.[202] The wife fully consented to the searching of a password-protected computer located in a common area of the house primarily used by the husband.[203] Based on the apparent authority of the wife, the court refused to suppress the results of the search.[204] The court acknowledged that the husband, "[b]y using a password . . . affirmatively intended to exclude . . . others from his personal files."[205] When the officers entered the home to seize the computer, it was on and visibly lit.[206] Nevertheless, without looking for password protection or "any information on the computer," the officers proceeded to shut down the computer and take it with them for forensic analysis.[207] Furthermore, the

---

[197] *Id.*

[198] *Id.* "The eraser program eliminated much of the evidence of Defendant's viewing of child pornography, but for some unknown reason, the program did not delete . . . approximately 148 images . . . recovered from the computer." *Id.*

[199] The court also concluded that because the wife was able to (essentially) sneak onto her husband's computer to install the spyware software, she therefore in fact had access to the computer to support an officer's reasonable belief in her apparent authority to conduct a warrantless search. *Id.* at 664.

[200] *Id.* at 663-64 ("If apparent authority existed at that time, later-discovered facts that might undermine the initial reasonable conclusion of third-party apparent authority are generally immaterial.").

[201] 473 F. 3d 551 (4th Cir. 2007).

[202] *Id.* at 553.

[203] *Id.*

[204] *Id.* at 555-56. In a footnote, the court declared that it was not deciding on the intentional avoidance of password discovery: "We do not hold that the officers could rely upon apparent authority to search while simultaneously using mirroring or other technology to intentionally avoid discovery of password or encryption protection put in place in by the user." *Id.* at 556 n.3.

[205] *Id.* at 554. The court went on to say, in a manner consistent with what one would think would lead to a suppression of the evidence, "it can not be said that . . . [the husband] . . . assumed the risk that a joint user of a computer, not privy to password-protected files, would permit others to search his files." *Id.*

[206] *Id.* at 553.

[207] *Id.*

government indicated that its "forensic analysis software would *not necessarily* detect user passwords."[208] Even though the wife admitted she did not know much about the computer, the court further validated the admittance of the evidence by putting the onus on the wife for not indicating to the officers that passwords may have been present.[209]

In this case, we see the court struggling with passwords as "locks," as well as what information officers should know. However, instead of requiring officers to ask minimal and appropriate questions to obtain a basic grasp of the surrounding circumstances, this court places the blame on the third-party wife for not informing the officers about any passwords. Somehow, the court arrived at a conclusion that effectively places an expectation on the layperson to perform the duties of law enforcement personnel.

B. The Andrus *Court Swings for the Fences*

In *Andrus*, federal law enforcement had been investigating and surveilling Ray Andrus, including his home and his work, for eight months on suspicion of child pornography.[210] After such surveillance, officers did not believe they had enough information to obtain a warrant and proceeded to conduct a "knock and talk."[211] The police officers specifically brought a forensic computer expert with them to the Andrus home.[212] Ray Andrus's 91-year-old father greeted the officers at the door in his pajamas and allowed them into his home.[213] The home belonged to the father, and Ray Andrus had his own bedroom while he lived there to take care of his aging parents.[214] Ray Andrus's private bedroom contained the only computer in the house.[215] The father consented to the search of the computer.[216] The police expert used forensic software to bypass password protection on the computer and found files depicting child pornography.[217] Only after the search returned results did the

---

[208] *Id.* (emphasis added).

[209] *Id.* at 555.

[210] United States v. Andrus, 483 F.3d 711, 713 (10th Cir. 2007). Authorities first became aware of Ray Andrus while performing an investigation into a third-party credit card billing company. *Id.* This company "provided subscribers with access to websites containing child pornography." *Id.* Credit card information led the authorities to Ray Andrus after the authorities found that "[t]he Andrus . . . subscription was used to access a pornographic website called www.sunshineboys.com." *Id.*

[211] *Id.*

[212] *Id.*

[213] *Id.*

[214] *Id.*

[215] *Id.*

[216] *Id.*

[217] *Id.* at 714. The court explained that "[the forensic expert] . . . used [forensic software] to search for . . . picture files. He explained that clicking on the images . . . allowed him to see the pathname for the folders on the computer's hard drive. This. . . . revealed . . . file names suggestive of child pornography. [He] estimated it took five minutes . . . ." *Id.*

police officer halt the forensic search on the grounds that a continuing conversation with the father indicated he might not have the authority to consent.[218]

In deciding on the admissibility of the evidence in *Andrus*, the court recognized that a computer with password protection is like a locked suitcase or briefcase.[219] The court analogized to *United States v. Block*,[220] where that court held a mother lacked authority to consent to the search of her son's locked footlocker when she did not have the key.[221] The court further analogized the situation to *Trulock v. Freeh*,[222] where that court held that although a third party had consent to a general search of the computer, that authority did not extend to the defendant's password-protected files.[223] Furthermore, the *Andrus* court looked at instances where the location of the computer in the house played a role in determining third party-consent.[224] The court recognized that when the computer is in a common area of a house, there is a more reasonable basis for officers to believe that the third party had "apparent authority" to consent to the search.[225] The court went on to say that "a personal computer is often a repository for private information the computer's owner does not intend to share with others."[226] With all this authority the court cited going in favor of suppressing the evidence, they nevertheless allowed admittance of the evidence.[227]

---

[218] *Id.*

[219] *Id.* at 718 (citing United States v. Aaron, 33 F. App'x 180 (6th Cir. 2006) (unpublished) and Trulock v. Freeh, 275 F.3d 391 (4th Cir. 2001)).

[220] 590 F. 2d 535 (4th Cir. 1978).

[221] *Id.*

[222] 275 F.3d 391 (4th Cir. 2001).

[223] *Id.* at 403.

[224] United States v. Andrus, 483 F.3d 711, 719 (10th Cir. 2007).

[225] *Id.* at 719-20.

[226] *Id.* at 718. The court emphasized its point by stating:

> [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.

[227] *Id.* at 722. Perhaps at least one underlying reason for the admittance of the evidence in this case, whether in the conscious or subconscious of the court, is the struggle between liberty and justice. While certainly beyond the scope of this Note, that struggle certainly weighs upon the courts. Often, the "motivation for these decisions has been the link between judicially acknowledging a violation of Fourth Amendment privacy and suppressing reliable, incriminating evidence." Sherry F. Colb, *What is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 121 (2002). This can certainly help to provide an explanation where some court decisions seem to reduce the protections of the Fourth Amendment. *Id.* "In other words, because a holding that the Fourth Amendment applies in a particular case might free a guilty defendant, courts are tempted to find no Fourth Amendment application." *Id.*

Setting aside the glaring problems of the officer not even asking questions appropriate to determining the 91-year-old father's authority to consent, or that the officer did not even so much as look for a password, the evidence would seem to show that Ray Andrus satisfied the two-prong test associated with Fourth Amendment protection analysis.[228] First, the court itself cited case law to show that Ray Andrus had a subjective expectation of privacy when he password-protected his computer and kept it in a non-common area of the house—his own private room.[229] Second, as to the objective—or what society would deem as reasonable—test, the court flat out declared that computer owners believe that their computers are private and do not intend to share private information with others. [230] So how did the court find a way to let the evidence in? By allowing law enforcement to play dumb.

The court put forth a myriad of explanations and reasons as to why they let the evidence in, even though, as mentioned above, the court itself so much as declared that Ray Andrus met the two-pronged test of Fourth Amendment analysis. Essentially, the court looked to not only the reasonableness of the officer's belief in the father's authority to consent, but also the "mysterious witchcraft" of computers and passwords. While acknowledging that officers did not ask specific questions about the elderly father's use of the computers, the court blamed the father for not indicating that he *did not* use the computer.[231] The court further declared that if the situation looked reasonable, the officers did not need to ask clarifying questions.[232] And although the court went to great lengths to compare the password-protected computer to a "locked box" requiring a key, they held that determining the existence of the password was unnecessary, because it would not have been "obvious" to the officers.[233] Furthermore, the court said that even though the computer required a password, there was nothing that showed the officers "knew or had reason to believe" a password was in place.[234]

These holdings create the absurd result of extending "apparent authority" to an almost infinite end. They allow police officers to skate around the Fourth Amendment by intentionally avoiding asking questions of third parties while obtaining consent, as well as allowing them to ignore password "locks" on

---

[228] *See supra* note 38 and accompanying text.

[229] *See generally Andrus*, 483 F.3d 711 (citing case law to demonstrate there was no authority to search).

[230] *Id.* at 719-20.

[231] *Id.* at 720.

[232] *Id.* The court then dismissed the dissent's argument that such an inquiry would be minimal. *Id.*

[233] *Id.* at 718. The court declares:

> Unlike footlockers or suitcases, where the presence of a locking device is generally apparent by looking at the item, a "lock" on the data within a computer is not apparent from a visual inspection of the outside of the computer, especially when the computer is in the "off" position prior to the search.

Id.

[234] *Id.* at 721.

computers that, as shown, courts have held to be analogous to locks on physical items.

VII. BRINGING THIRD-PARTY CONSENT OF WARRANTLESS COMPUTER SEARCHES BACK UNDER FOURTH AMENDMENT PROTECTION

While warrantless computer searches conducted by third-party consent may be more of the exception than the norm,[235] holdings such as the ones in *Andrus* open up the floodgates of potential Fourth Amendment violations in this area. The solution is not to change the standard, but if courts are going to liken password-protected computers to locked boxes, it is imperative that they consistently apply those principles instead of dancing around it and allowing evidence in based on what is "reasonable under the circumstances." The fact is that computers are in a majority of American homes.[236] It is not acceptable to allow law enforcement to act as though they have no idea computers come with password protection. The fact that law enforcement has forensic technology to purposely avoid password protection[237] negates the contention that willful blindness towards passwords is acceptable.

Had the court in *Andrus* applied both the two-prong reasonable expectation of privacy test and the limits on apparent authority rationale to the warrantless password-protected computer search in a manner consistent with Fourth Amendment law as applied to similar scenarios, the exact opposite outcome would have resulted. It is both counter-productive and counter-intuitive to the legal system to declare that passwords on computers are analogous to locks on boxes, and then state that law enforcement has no duty to even ask or look to see if password-protection is present. If Ray Andrus's room would have been locked, and the father did not have a key, the police officers would not have been able to enter the room. Simply put, a locked container supports a heightened expectation of privacy when a potential third-party consenter has no ability to provide a key to the lock on that container.[238] Third-party authority in these cases is far from apparent. A third party has "no right . . . to consent to a search of personal property belonging to another person unless there is evidence of both common authority over and mutual usage of the property."[239] Furthermore, "when police are told by a third party that the property belongs to another, the officers are obligated to make inquiries sufficient to establish that the person consenting to the search has both common control over the property and mutual use of it."[240]

Not requiring law enforcement to ask appropriate questions simply because the device is a computer steps on the very protection the Fourth Amendment is designed to provide. If law enforcement, in searching a physical container with third-party consent, used an X-ray machine to see the contents without so much as even looking

---

[235] *Id.* at 722 n.1 (McKay, J., dissenting).

[236] *See* Households with Computers: 1998 and 2003, *supra* note 107 and accompanying text.

[237] *See* Thompson, *supra* note 89 and accompanying text.

[238] *Andrus*, 483 F.3d 711 (reiterating cases finding a privacy interest).

[239] Marganet v. State, 927 So. 2d 52, 57 (Fla. Dist. Ct. App. 2006).

[240] *Id.* at 58.

at the front to see if a lock was present, any court would suppress the evidence. In theory, the same should hold true for personal computers. The argument that password protection on a computer may not be "immediately visible" lacks support. Simply turning on the machine shows whether password protection is enabled. Furthermore, the fact that a third-party consenter does not know if there is password protection is stark evidence to the contrary that he or she has any authority at all over the computer.

A common sense, reasonable solution to the problem of warrantless computer searches based on third-party consent consistent with established principles is two fold: (1) Require officers to make minimal inquiries to the third party as to the ownership of the computer and what access he or she has to the computer system, and (2) Require officers, at a minimum, to turn on the computer to check for password protection.

What may seem like reasonable solutions are exactly what the court in *Andrus* indicates are unreasonable. The burden of officers to find out if the third party has anything to do with the computer in question is minimal.[241] Officers are only required to ask questions when the situation is ambiguous. In this context, similar questions that determine common ownership and access rights to physically locked items can be presented to the third party. Questions such as "Do you use this computer" and "Do you have the password (key) to log on to the computer?" are hardly a burdensome task for an officer, especially when it comes to protecting Fourth Amendment rights. Allowing law enforcement to "rely" on the surrounding circumstances in these cases is overly broad, especially when the courts are going to place the blame on the third party for not being the first to mention that there is password protection.

Further, it is not a burden on law enforcement to require them to look for the presence of a password prior to forensically extracting data. Surely no court has allowed evidence to stand where an officer could not "see" the lock on a physical container and cut a hole in the side to remove the contents. To indicate that not seeing a password negates the need to check for one is equally as disturbing as not requiring the asking of minimal questions to establish common authority. As Judge McKay put it in her dissent in *Andrus*, "the facts that a computer 'lock' may not be immediately visible does not render it unlocked."[242] Simply requiring law enforcement to exercise due diligence by turning on the computer to look for a password will help solve this problem.

As technology continues to play a bigger role in daily life, placing such minimal restrictions on law enforcement is consistent with Fourth Amendment principles of reasonableness. It also allows for the striking of a balance between the government's interest in protecting and serving society as a whole with the individual's right to privacy. While the Fourth Amendment warrant requirement may be riddled with exceptions such as third-party consent, it must not be forgotten that "the fourth amendment is quintessentially a regulation of the police—that, in enforcing the

---

[241] United States v. Andrus, 483 F.3d 711, 724 (10th Cir. 2007) (McKay, J., dissenting).

[242] *Id.* at 723 (McKay, J., dissenting). "[U]nlike the locked file cabinet, computers have no handle to pull. But, like the padlocked footlocker, computers do exhibit outward signs of password protection: they display boot password screens [and] username/password log-in screens." *Id.*

fourth amendment, courts *must* police the police."[243] In that vein, placing reasonable restrictions on police when they are performing their duties is certainly not a new concept. For example, when a suspect is lawfully arrested in his vehicle, police may search the passenger compartment of a car and any containers therein because those areas are within the immediate grabbing area of the arrestee and may contain a weapon.[244] However, police cannot search the trunk.[245] Furthermore, if there is no arrest, but just a citation, there can be no searching simply based on that citation.[246] Even the "plain-view rule," which allows police to seize immediately recognizable contraband or evidence of a crime cannot be used to justify warrantless searches or seizures. Restrictions on the plain-view doctrine require police to be lawfully in the position from which they see the item, and prohibits further examination of the item unless it is immediately recognized as something unlawful.[247] All of these are reasonable restrictions and safeguards designed not only to aid police, but also to enforce the requirements of the Fourth Amendment and ensure individual privacy.

Establishing rules for police conduct, which go as far as possible to ensure their safety as well as protect individual privacy, is also present in another type of warrantless search—those occasions where police patrolling the street believe crime to be afoot. In *Terry v. Ohio*,[248] the U.S. Supreme Court upheld the practice whereby a police officer can stop a suspect based on reasonable suspicion that he has or is about to commit a crime, briefly detain him, ask questions, and perform a limited search on the person to see if he is carrying a weapon.[249] While the overarching principle in allowing the limited search is the officer's safety, the search is just that—limited. The officer may only perform a pat down/frisk on the exterior of the clothing. If no questionable objects are felt, the officer may not go digging into the pockets of the suspect.[250] While many may have seen this as an expansion of police power, the restrictions on the police are reasonable—limited detention, questioning, and searching. The police know what their boundaries are in that type of situation. Similarly drawn boundaries are also now required in terms of warrantless searches of password-protected computers based on third-party consent. Otherwise, there lacks an objective basis through which courts can accurately assess the constitutionality of such intrusions.

A locked container shows a manifestation of an expectation of privacy. The fact that something is locked provides a limit to any authority that a third-party consenter may have. Asking a couple questions about a computer, a practice commensurate with establishing authority over physical objects with locks on them, is a non-

---

[243]Tracey Maclin, *When the Cure for the Fourth Amendment Is Worse than the Disease*, 68 S. CAL. L. REV. 1, 6 (1994) (emphasis added).

[244]New York v. Belton, 453 U.S. 454, 460 (1981).

[245]*Id.* at 461 n.4.

[246]Knowles v. Iowa, 525 U.S. 113, 118 (1998).

[247]Arizona v. Hicks, 480 U.S. 321, 327-29 (1987).

[248]392 U.S. 1 (1968).

[249]*Id.* at 30.

[250]*Id.*

burdensome way to uphold the protections of the Fourth Amendment. Law enforcement should not be able to sidestep the protections of the Fourth Amendment because the virtual world can be searched with technology that bypasses locks.

VIII. CONCLUSION

The very words of the Fourth Amendment require a warrant to conduct a search or seizure. The Supreme Court has recognized that "the possession of a warrant by officers conducting [a] . . . search greatly reduces the perception of unlawful or intrusive police conduct, by assuring the individual whose property is searched or seized the lawful authority of the executing officer, his need to search, and the limits of his power to search."[251] Relying on the apparent authority of a third party to consent to the search of a password-protected computer can seriously infringe on the right to be free from warrantless searches and seizures. The few court decisions that have touched on the topic apply a liberal standard. Whether that stems from a fear or misunderstanding of technology, the results amount to skating around the protections guaranteed by the Fourth Amendment. Regardless, law enforcement's use of forensic technology specifically designed to bypass passwords negates the contention that officers can be oblivious to the existence of password-protected computers. Requiring officers to ask minimally burdensome questions of the third party, as well as physically checking for the existence of a password, will bring this area of the law back into accord with the established principle that law enforcement cannot rely on the consent of a third party to search a locked area when that third party does not have a key.[252] Clearly, requiring anything less in an increasingly technology-filled society results in a grave deprivation of the very protections the Fourth Amendment is designed to provide.

---

[251] Illinois v. Gates, 462 U.S. 213 (1983).

[252] United States v. Block, 590 F.2d 535 (4th Cir. 1978).