Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 19 *Volume XIX*
Number 1 *Volume XIX Book 1*

Article 4

2008

The Continuing Evolution of Consent and Authority in Digital Search and Seizure

Aaron Stanley
Fordham University School of Law

The Continuing Evolution of Consent and Authority in Digital Search and Seizure

Cover Page Footnote

For Elmer—who continues to inspire me to learn something new every day. Many thanks are due to the Fordham IPLJ editorial board and staff and the team at Stroz Freidberg who brought me into the world of digital forensics. I greatly appreciate the support and assistance of Luke Cats, Manoj Choudhary, and my family.

The Continuing Evolution of Consent and Authority in Digital Search and Seizure

Aaron Stanley*

> "Privacy is not something that I'm merely entitled to, it's an absolute prerequisite."
>
> —Marlon Brando[1]
>
> "[T]here is nothing new in the realization that the Constitution sometimes insulates the criminality of a few in order to protect the privacy of us all."
>
> —Antonin Scalia[2]

A PDF version of this article is available online at http://law.fordham.edu/publications/article.ihtml?pubID=200&id=2884. Visit http://www.iplj.net for access to the complete Journal archive.

* J.D. Candidate, Fordham University School of Law, 2009; B.A., New York University, 2000. For Elmer—who continues to inspire me to learn something new every day. Many thanks are due to the Fordham IPLJ editorial board and staff and the team at Stroz Freidberg who brought me into the world of digital forensics. I greatly appreciate the support and assistance of Luke Cats, Manoj Choudhary, and my family.

1 QuotationsBook—Brando, Marlon Quote, http://quotationsbook.com/quote/32444 (last visited Oct. 28, 2008).

2 Arizona v. Hicks, 480 U.S. 321, 329 (1987).

INTRODUCTION

Even though very few Americans live alone, most of us keep secrets. The United States Constitution guarantees that, absent a probable cause determination, our secrets will remain unseen, unheard, and unknown by those from whom we wish to conceal them.[3] The Supreme Court has seen fit to draw a few exceptions

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

to the search warrant requirement, and one of those is based on consent.[4] An individual who wishes to cooperate with the police and waive the requirement that officers obtain a warrant before executing a search of her apartment is free to do so at her own risk. The Court has recognized a number of rationales for this exception, but also certain caveats.[5] This Note explores the law of the consent-search exception and some of the technological challenges that make its application more difficult.

Assume, for the purposes of this Note, that the FBI suspects George Costanza is involved in an identity theft ring. Given that identity theft is a crime made much easier by modern technology, there is a good chance that George's computer contains e-mail and other information that will confirm the agents' suspicions. Surveillance by the FBI has neither provided enough evidence to obtain a search warrant for George's house nor a wiretap. George lives with, and takes care of, his elderly mother in a home that she owns. Hoping to catch a break, the agents visit George's home while he is at work and ask his mother whether she would consent to a search of the home for evidence of George's involvement in the identity theft ring. George's mother allows the agents to look around. In the course of their search, and much to their surprise, the agents discover a banker's box full of printed documents that implicate George in the identify theft ring. The box (which had no lid on it, oddly) was sitting on the floor in a closet to which George's mother had unfettered access.

Provided that the consent was properly obtained and not coerced, does such a search violate George's constitutional rights? The scenario seems straightforward, and it is unlikely that George would succeed in arguing that the agents unconstitutionally invaded his privacy. If the hypothetical documents were stored on a computer, however, despite the fact that both a computer and a banker's box are essentially storage devices, is there something special about the way the documents are stored that changes the reasonableness of the search? Many courts have recognized that there are substantial differences between the computer and the box,

---

4 Mitchell Waldman, AM. JUR. 2D *Computers and the Internet* § 21 (2008).

5 *See id.*

yet the doctrine remains relatively the same for digital and physical evidence.[6]

In January of 2004, the federal government began investigating Ray Andrus.[7] As a result of the investigation, and the trial court's denial of his motion to suppress evidence recovered from a computer, Mr. Andrus pled guilty to charges of possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B).[8] Mr. Andrus lived with his parents, just like George Costanza above, and the evidence was recovered from a computer kept in his bedroom.[9] And also similar to George's case, it was Mr. Andrus' father who consented to the search of the computer while his son was away from the home.[10] On appeal to the Tenth Circuit, Mr. Andrus argued that the search was improper for a number of reasons, but ultimately the court, treating the computer very much like a banker's box, held in favor of the government over a short, but intriguing dissent by Judge McKay.[11]

Mr. Andrus argued unsuccessfully that, because the computer was configured to require each user to logon with a unique password, the police should not have searched through files that were contained on the hard drive under his user profile folder.[12] To bring this argument somewhat in line with George's case, suppose that George had, instead of storing just loose papers in the banker's box, used manila envelopes to separate his papers from his mother's. The envelopes are not really secured, since anybody with access to the box could easily open each envelope and read the paper inside, but George marked the envelopes so his mother would know where not to look. Likewise, George doesn't intrude

---

6 *See, e.g.*, Trulock v. Freeh, 275 F.3d 391 (4th Cir. 2001) (discussing how the Fourth Circuit has recognized that computer files should be treated with a high degree of privacy protection, but generally looks at computers as physical devices); *see also* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 538–40 (2005) (discussing the unique features of the computer hard drive as a file storage mechanism).

7 United States v. Andrus (*Andrus*), 438 F.3d 711, 713 (10th Cir. 2007), *reh'g en banc denied*, 499 F.3d 1162 (10th Cir. 2007).

8 *Id.* at 712.

9 *Id.* at 713.

10 *Id.* at 712–14.

11 *Id.* at 711–25.

12 *Id.* at 715–22.

on his mother's private storage area. Admittedly, this analogy is weak because it doesn't encompass the complexities of the security features the computer user is capable of implementing, but that is part of the reason why computers *are* in fact different from other storage devices.

And this is where the incredibly significant and terribly difficult conceptual difference between the physical evidence in George's case and the digital evidence in Mr. Andrus's case becomes a hard legal question. The specifics of how the files stored on the computer differ from those stored in the banker's box are discussed in detail below, but it is important to understand at the outset of this discussion that there are no real analogs in the world of physical evidence to the ways in which one can protect data on a computer.

Today, computer users generally use passwords to control access to data, but fingerprints and other biometric mechanisms are slowly being adopted as replacements. Users and software manufacturers have begun to take security more seriously, and users are starting to exert more control over their data in an effort to keep hackers and identity thieves from hurting them. Mr. Andrus's use of a password was intended to keep others from accessing his private data. In his case, however, it was as effective as George writing "Do Not Open: George's Stuff" on a manila envelope containing his contraband.

As the doctrine of consent searching has evolved, so has the evidence it seeks to uncover and the technologies used by police to find that evidence. This Note explores the doctrine of consent searching as it applies specifically to evidence recovered from a computer that is shared among multiple members of a household.[13] Part I provides the relevant background information on the current state of computer technology vis-à-vis the two major operating

---

[13] For the purposes of this Note, members of a household could, but need not be related. While there may be a slightly different analysis if the co-inhabitants are married, those issues are beyond the scope of this Note. For an overview of how a spousal relationship may be treated differently, see U.S. DEP'T OF JUSTICE COMPUTER CRIME & INTELLECTUAL PROP. SECTION CRIMINAL DIV., SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS (July 2002), *available at* http://www.cybercrime.gov/s&smanual2002.htm [hereinafter DOJ MANUAL].

systems in wide home use, the software that police use in forensic examinations of computer systems, and the scholarship and case law relevant to the discussion. In Part II, the article moves to a discussion of the two-pronged debate which surrounds the searching of computer systems pursuant to consent by one of the computer's users, which was most recently highlighted in *United States v. Andrus*.[14] Finally, Part III sets forward a framework within which law enforcement agents can simultaneously achieve their goals and maintain the privacy protections the Constitution requires.

I. BACKGROUND

A. Observations About the State of Home Computing

More and more our modern lives require us to own and use many different types of technology. The mobile phones that allow teenagers to constantly send text messages to each other in lieu of actual conversation are more powerful than the family computers of the early 1990s. Though it may have been forced to endure many upgrades, the family computer remains a requirement for most. Microsoft still, as it has for many years, dominates the operating system market, and most home computers run some version of Microsoft's Windows operating system.[15] In recent years, Apple has secured a larger portion of the market, which means that any home computer that might be the target of police investigation will more probably than not run Windows or the Mac OS.[16] Due to concerns that many users have expressed over the security of

---

[14] *Andrus*, 438 F.3d at 722.

[15] OneStat Website Statistics and Website Metrics, http://www.onestat.com/html/aboutus_pressbox46-operating-systems-market-share.html (last visited Sept. 9, 2008).

[16] As of the writing of this Note, the operating system shipped with all new Apple computers is called Mac OS X. *See, e.g.*, Apple—Get a Mac—Why a Mac, http://www.apple.com/getamac/whymac (last visited Sept. 13, 2008). Sometimes it is referred to as System X (roman numeral ten) because the version of the operating system immediately preceding it was System 9. *See* Posting of Rich Brown to Crave Blog, http://news.cnet.com/8301-17938_105-9936378-1.html (May 5, 2008, 2:51 PM PDT); *see also* Wikipedia—Mac OS, http://en.wikipedia.org/wiki/Mac_OS (last visited Sept. 13, 2008).

their computer files, both operating systems have been designed from the ground up with security in mind.

Microsoft Windows XP is the most common operating system in use today, and it was designed specifically to be a multi-user home computer operating system.[17] Microsoft envisioned XP as the hub of digital life and the digital family, and as such incorporated design features that would make multi-user operation simple.[18] The hallmark of multi-user computing is some division of computer resources among the users of a computer. Users of parallel-processing supercomputers and mainframes may know that resources are normally divided up based on the amount of CPU time[19] that will be needed to complete a given operation, but the home PC environment is structured quite differently. At home, family members generally interact with the computer one at a time, and so a simple division of space on the computer's hard drive suffices to allocate the computer's resources. But to access these individual allocations, Mom, Dad, and each of the kids need to have his or her own username. Both Windows and the Mac OS allow multiple usernames on the same computer, and users are required to authenticate, normally with a password, in order to access the files stored within their allocation on the computer.

During the initial setup phase of the operating system, which happens when the end-user first powers on the computer, both Windows and Mac OS requires the user to set a password for his or

---

[17] According to a recent survey, many corporate workstations run Windows XP. Gregg Keizer, *Vista's Biggest Problem Remains Windows XP, Survey Says*, PC WORLD, Nov. 14, 2007, http://www.pcworld.com/article/139664/article.html. Home users have been reluctant to upgrade to Microsoft Windows Vista from XP, believing that XP is a more stable operating system. *See* Harry McCracken, *Windows XP vs. Vista: An Explosion of Opinion*, PC WORLD, Mar. 20, 2008, http://www.pcworld.com/article/143414/windows_xp_vs_vista_an_explosion_of_opinion.html. According to a study conducted in 2006, Windows XP has a "global usage share of 86.80 [%]." OneStat Website Statistics, *supra* note 15.

[18] *See* Jim Hu & Mike Ricciuti, *Gates Takes Wrap Off Windows XP*, CNET, Oct. 25, 2001, http://news.cnet.com/2100-1001-274939.html.

[19] CPU Time is "[t]he amount of time the CPU is actually executing instructions." What is CPU Time?—A Word Definition from the Webopedia Computer Dictionary, http://www.webopedia.com/TERM/C/CPU_time.html (last visited Oct. 28, 2008); *see also* Wikipedia—CPU Time, http://en.wikipedia.org/wiki/CPU_time (last visited Aug. 25, 2008).

her account.[20] The user may then create as many additional accounts as needed and set a unique password for each of them. Even outside of the operating system itself, passwords are a part of life for computer users, as most major web sites require users to register in order to read articles, buy goods, or simply interact with the site.

There are two main exceptions to the general rule that multiple user accounts on today's common home computers will have user-assigned passwords. The first is that some users enable the auto-logon feature of their operating system, eschewing multiple user accounts for one family account.[21] Such a configuration means that Mom, Dad, and all the kids share access to all Internet bookmarks stored by the web browser, e-mail account profiles in the e-mail reader, and all settings in the various programs. When such a configuration is chosen, the account will usually be setup to logon automatically when the computer starts. Such configurations are much more common, however, with computers operated by single users, as opposed to in a multi-user environment.[22] One important technical question is whether it is possible, and feasible, to identify these different configurations before conducting a search of the data stored on the computer.

The second exception where multiple users may share a computer without individual passwords is a situation in which the computer's administrator has configured the accounts such that users cannot change their passwords.[23] This is a common configuration in a corporate environment where multiple employees work different shifts at the same stations. It may also present itself in educational settings or even at home where a parent wants to maintain access to a child's account to monitor his or her activity.[24]

---

[20] This initial account will be a computer administrator and provide "full control of the PC . . . ." Windows XP, http://itproxy.org/pcguide/msos/winxp.htm (last visited Oct .28, 2008).

[21] *See, e.g.*, Mark Kaelin, *Set Up an Automatic Logon to Windows XP*, TECHREPUBLIC, May 4, 2004, http://articles.techrepublic.com.com/5100-1035_11-5280112.html.

[22] *See id.*

[23] The administrator creates the username and password, thus making the account private. Windows XP, *supra* note 20.

[24] This scenario is analogous to a situation where the unlocked child's room contains a locked dresser, but the parent has a key and unlocks it before the police search through it.

The recommended configuration for a family computer, despite the possibility for alternatives, is to configure the computer with separate accounts for each family member so that they may maintain their independent bookmarks, e-mail, and data.[25] One user may further expect that if she has a unique password for her account, the other family members will not be able to access her data unless she divulges the password to them.[26] The security features of the operating system generally prohibit one user from accessing another user's data folders unless that user has explicitly given permission to the other.[27] Granting other users permission to access data is possible with both Windows and the Mac OS, but by default each user's data will be protected from prying eyes.

In the common multi-user configuration, each user account is linked to specific folders on the computer that are used for data storage.[28] On a Windows PC, these folders can be found in the "Documents and Settings" folder, located in the root directory of the hard drive. If one user were to open the main "Documents and Settings" folder, she would see folders created for each additional user on the system but, unless she had been given special security privileges by the folder's owner, she would not be able to open any folder but the one linked to her account. The operating system maintains a certain amount of metadata that relates to the permissions for each file and folder.[29] When an unauthorized user at-

---

In that regard, the situation mentioned above is outside the technical bounds of this Note; however, the investigative principles laid out in the Conclusion, if followed, would effectively discover the configuration and allow the agents to work within the bounds of the Constitution while eliminating the possibility of a challenge to their search. For a discussion of the differences between physical and computer searches, see Kerr *supra* note 6, at 538–50.

25 Tips to Protect Kids Online—Microsoft Security, http://www.microsoft.com/protect/family/guidelines/basics.mspx (last visited Oct. 28, 2008).

26 Users have the option of configuring their accounts as "private" which makes them "inaccessible to other users." Windows XP, *supra* note 20.

27 *See id.*

28 *Id.*; s*ee also* Wikipedia—User Profile, http://en.wikipedia.org/wiki/User_profile (last visited Sept. 9, 2008).

29 Metadata, in this context, means the information which is not a part of the file itself but rather is tracked by the operating system for purposes of file management, specifically security. Chris Taylor, An Introduction to Metadata (July 29, 2003), http://www.library.uq.edu.au/iad/ctmeta4.html; *see also* Wikipedia—Metadata, http://en.wikipedia.org/wiki/Metadata (last visited Sept. 9, 2008).

tempts to open a document for which she does not have permission, the operating system interrupts the request and denies the user access. Based on the way the operating system functions to protect the user's data, she may expect that her files are secure and will remain private.[30]

B. Why Digital Evidence Poses Unique Problems

In the time before the atom, what we could see with our eyes was all there was. Similarly, when the country was young and the universe of searchable data was limited to "papers, and effects," law enforcement agents were able to literally *see* everything covered by Fourth Amendment protections.[31] As technology has developed, however, the fundamental building blocks of data have changed. As the discovery of the atom gave way to a whole new world of life, the use of bits, bytes, hard drives, and computers has provided many challenges for search and seizure law.

The most interesting, and legally problematic, feature of computer-based evidence is that it can be classified both physically and logically. One can look at the data contained on a computer from two very different perspectives, and the choice to treat the evidence one way or the other can lead to very different legal outcomes. In his article addressing this dichotomy, Professor Orin Kerr examined a number of the different considerations that must be addressed before deciding which perspective to adopt.[32] On one hand, the computer's hard drive, like the computer itself, is a physical piece of equipment. Despite the fact that the courts routinely do so, however, analogizing the hard drive to any other piece of physical evidence ignores its unique characteristics.[33] Kerr identified four main differences between computer evidence and

---

[30] The Mac OS has a similar scheme for organizing data. For a detailed description of how the operating system is organized, see An Introduction to Mac OS X Security for Web Developers, http://developer.apple.com/internet/security/securityintro.html (Oct. 28, 2008).

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

[32] Kerr, *supra* note 6.

[33] *See* United States v. Andrus, 483 F.3d 711, 718 (10th Cir. 2007), *reh'g en banc denied*, 499 F.3d 1162 (10th Cir. 2007); *see also* Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir. 2001).

traditional physical evidence: first, searches of computer evidence normally occur outside of the place being searched; second, investigators can create exact duplicates of seized hard drives; third, hard drives have immense capacity, well beyond any other physical device; and fourth, there are procedural technicalities that make searching a hard drive far more difficult than searching other physical evidence.[34]

How the courts equate files to "papers" can mean a world of difference in a criminal case.[35] Thinking back to the banker's box hypothetical, assume that there were different folders for each victim in the identity theft ring stored in the box. Generally, we could think of each folder as containing a "file" pertaining to one of the victims. In this case, a file is a compilation of papers stored within a container, the folder.[36] It is equally valid, however, to think of each individual piece of paper as a file stored within the container of the folder. These different conceptions of how to apply the word "file" in the physical wolrd are really semantic, but in the digital world the name given to a particular block of data can have enormous consequences.[37] These distinctions are critically important in determining whether the scope of one party's consent has been exceeded by the search.

In judging the reasonableness of a consent search, courts must examine the scope of the original consent. The scope of a search of someone's home "is largely intuitive; it correlates neatly with what is hidden and what is exposed."[38] Unlike a physical search where once the closet door is opened the banker's box is visible to everyone, in the digital world, where files can have individual se-

---

[34] Kerr, *supra* note 6, at 538–47.

[35] *Id. But see* Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L.J. 193, 198 (2005) (arguing that evaluating the legality of searches and seizures of computer evidence need not be any different from evaluating the legality of paper searches).

[36] Kerr analogizes folders to zippered pockets within a briefcase. Kerr, *supra* note 6, at 555.

[37] *See id.* at 554 (discussing the differences between the logical and virtual approaches to looking at data contained on a hard drive). By treating the data contained on a hard drive as a virtual file cabinet, each individual folder and/or file can have specific security properties in addition to the properties set for the entire drive. *Id.*

[38] *Id.*

curity settings or be situated such that one user may not normally be able to access them, what is exposed in plain view to one user may be hidden to every other user. But there are technologies that allow computer technicians to expose certain areas of a hard drive where data might normally be invisible to one or a group of users.[39]

In a typical investigation where computers are seized, the evidence may be collected from one location and then transported to another for the actual search.[40] When law enforcement officers conduct a search of a home, they are generally looking for evidence which they can discern as relevant based on physically observable characteristics. Because the data stored on a hard drive cannot be identified without the use of a computer, the act of searching the drive normally does not occur on-site, but at the investigators' own laboratory.[41]

C. Some Basics of The Forensic Investigation Process[42]

The well-equipped computer forensic investigator has many tools at her disposal that can be used to dig up information that computer users are trying to hide. Probably the simplest of these tools is a disk duplicator or imager. A trained investigator only works off of a copy of an original hard drive.[43] Unlike physical evidence that one would expect would be collected at a crime scene (e.g., blood, bullets, knives), a properly made copy of a hard

---

[39] There are many software programs that are designed to bypass the user-password protection on a computer for purposes of forensic analysis and maintenance. As noted by the court in *Andrus*, one such program is Guidance Software's EnCase program, which is a computer forensic analysis utility. United States v. Andrus, 483 F.3d 711, 719 (10th Cir. 2007), *reh'g en banc denied*, 499 F.3d 1162 (10th Cir. 2007). In addition, utilities like Technology Pathways' ProDiscover, AccessData's Forensic Toolkit, and a free program created by Brian Carrier called The Sleuthkit can all be used by a computer user to bypass user-level security features. *See* Forensic Toolkit, http://www.accessdata.com (last visited Oct. 28, 2008); Sleuth Kit and Autopsy, http://www.sleuthkit.org (last visited Oct. 28, 2008); Technology Pathways ProDiscover Computer Forensics, http://www.techpathways.com (last visited Oct. 28, 2008).

[40] *See* Kerr, *supra* note 6, at 551, 557.

[41] *See id.*

[42] Empirical research in support of this section was conducted by the author with the gracious help of Luke Cats, Vice President, Stroz Friedberg.

[43] Kerr, *supra* note 6, at 557.

drive can be relied upon as a complete and accurate representation of the original.[44] Since these copies are exact replicas of the original, investigators can use the copies for their analysis and thus not risk damaging the suspect's hard drive.[45] The forensic duplication process allows investigators to make an infinite number of lossless duplicates. Unlike a photocopy, there is no degradation in quality each time one of the copies is copied. These copies are generally called "images" or "bitstreams" and are created with disk imaging software or hardware.[46]

Many new computers sold today come with hard drives that can store over 320 gigabytes of data.[47] Considering that one gigabyte is approximately equivalent to 1,000 books,[48] a single computer could potentially store one percent of the books in the Library of Congress, far more than could physically be stored in the average house.[49] With that much data to search through, a typical computer forensic investigation can take much more time and be far more complex than searching for the equivalent physical evidence.[50]

To conduct and manage the search of a computer hard drive, the investigator will normally use a software suite specifically de-

---

[44] *See* Equity Analytics, LLC v. Lundin, 248 F.R.D. 331, 334 (D.D.C. 2008) (noting that the general process of forensic duplication creates an identical copy of the original).

[45] *See id.*

[46] *See* Kerr, *supra* note 6, at 557; Wikipedia—Disk Image, http://en.wikipedia.org/wiki/Disk_image (last visited Aug. 25, 2008).

[47] *See, e.g.*, Apple—Mac Pro—Tech Specs, http://www.apple.com/macpro/specs.html (last visited Oct. 28, 2008); Gateway Official Site: Shop—Desktops—GT Series, http://www.gateway.com/systems/series/529598054.php (last visited Oct. 28, 2008).

[48] One gigabyte is approximately the equivalent of 300,000 pages of text or approximately five minutes of high-definition video. *See* LexisNexis Discovery Servs., How Many Pages in a Gigabyte? (2007), http://www.lexisnexis.com/AppliedDiscovery/lawlibrary/whitePapers/ADI_FS_PagesInAGigabyte.pdf; VideoSpace Online, http://www.videospaceonline.com (last visited Aug. 25, 2008).

[49] The Library of Congress contains more than 30 million books. General Information—About the Library, http://www.loc.gov/about/generalinfo.html#2007_at_a_glance (last visited Oct. 28, 2008).

[50] *See generally* Douglas A. Schmitknecht, *Building FBI Computer Forensics Capacity: One Lab at a Time*, 1 DIGITAL INVESTIGATION 177, *available at* http://www.rcfl.gov/Downloads/Documents/DigitalInvestigator.pdf; FED. BUREAU OF INVESTIGATION, REGIONAL COMPUTER FORENSICS LABORATORY ANNUAL REPORT FOR FISCAL YEAR 2007 34–67 (2007), http://www.rcfl.gov/downloads/documents/RCFL_Nat_Annual07.pdf.

signed for forensic analysis.[51] The market leader in this area is Guidance Software's "EnCase" product.[52] This software is, at its core, a very powerful search engine. It is designed to allow an investigator to examine every bit of data stored on a hard drive, including data the user may have deleted or otherwise tried to hide.[53] EnCase is able to read the data from an image of the original drive and display it in various ways.[54] Because there are many ways one can hide data on a computer hard drive, one of the most effective ways to use EnCase is to create a list of keywords that the software will search for, bit-by-bit, across the entirety of the hard drive.[55]

When an investigator uses the keyword search function, EnCase attempts to locate all instances of the specified words wherever they appear on the drive, whether they exist in active files, deleted files, or unused space on the drive. However, there is one notable limitation on this process. The software is generally unable to search through encrypted files or data.[56] If a user employs strong encryption to protect her data, the EnCase program will not be able to search anything except the metadata.[57] Home users are likely to rely on the operating system's password and account con-

---

51 *See* Kerr, *supra* note 6, at 544.

52 *See* Guidance Software, EnCase Forensic (2005), http://www.guidancesoftware.com/downloads/EnCase_Forensic.pdf; Guidance Software, http://www.encase.com (last visited Oct. 28, 2008).

53 Guidance Software, EnCase Forensic, *supra* note 52, at 2.

54 The term "image" is used interchangeably with "copy" or "bitstream." For a brief overview of the significance of this process, see Kerr, *supra* note 6, at 557–58.

55 When used in conjunction with a search warrant, EnCase can be an extremely powerful tool for locating the data for which the investigators have a warrant. There are limits even to those searches which are beyond the scope of this Note. For a more detailed discussion of the ways search warrants can be exceeded by EnCase, see Kerr, *supra* note 6, at 548–57.

56 Guidance Software, Encase Detail Products Description (2006), http://www.guidancesoftware.com/products/ee_index.aspx.

57 Strong encryption refers to any form of encryption algorithm that is mathematically difficult to attack. Generally, an algorithm which uses a key of greater than 128-bits is considered strong. *See* Encryption Level—Silly Dog 701, http://sillydog.org/netscape/kb/encryption.html (last visited Oct. 28, 2008); Wikipedia—Encryption, http://en.wikipedia.org/wiki/Encryption (last visited Aug. 25, 2008).

trols, rather than special data encryption software, to secure their data.[58]

EnCase is not just a glorified search engine; it is a full-featured forensic analysis suite with an extensive scripting language called EnScript.[59] One of the scripts included with the program is the "Case Processor" script.[60] This script, when executed by an investigator, will extract information about the computer system's configuration so that the investigator knows crucial details like which version of the operating system is installed, the time when the computer was last turned off and on, and the number and names of the user accounts active on the system.[61] The last of these is of critical importance. The Case Processor script provides the investigator with all of this information in a very short period of time.[62] The current version of EnCase includes additional investigative functionality that makes it very easy for an investigator to quickly determine what accounts have been created on the computer and whether there are passwords configured to protect those accounts.[63]

---

[58] A survey conducted by a user on ubuntuforums.org showed that an overwhelming majority of respondents did not feel a need to encrypt their data. Poll: How Many People Use Hard Drive Encryption?, http://ubuntuforums.org/showthread.php?t=661517 (last visited Aug. 25, 2008).

[59] Guidance Software, EnCase Forensic Detailed Product Description (2006), http://www.guidancesoftware.com/downloads/DetailedProductDescription.pdf.

[60] Guidance Software does not provide a public list of the EnScripts that are bundled with each version of the EnCase software, but this Note's author, while researching for this Note, used an out-of-the-box installation of EnCase version 6.5.1.2 which included the Case Processor EnScript. Screencaptures of EnCase version 6.5.1.2 are on file with this Note's author.

[61] Based on this Note's author's use of the Case Processor EnScript on EnCase version 6.5.1.2.

[62] A laboratory test of EnCase version 6.5.1.2 (conducted by this Note's author) showed that the Case Processor, executed on a 20 gigabyte Windows partition, takes approximately 30 seconds to identify and record all of the information. Screencaptures of EnCase version 6.5.1.2 are on file with this Note's author.

[63] Using EnCase version 6.5.1.2, an investigator can use the "User List" function available through the "Secure Storage" tab to identify all of the user accounts on the system. In addition to listing the users on the system, the "User List" function also displays a hash of the account's password, if there is one. For accounts that are not password-protected, this field is blank in the user list. Screencaptures of EnCase version 6.5.1.2 are on file with this Note's author.

Unlike encrypted data, however, these password-protected folders are easily searchable by EnCase.[64] Even though the program can be used to look at the metadata that tracks which users are allowed to access particular files, EnCase is not designed to respect those permissions. Investigators can use EnCase to search through files that are stored in places they would not otherwise be able to look. The software would, in essence, be crippled if it couldn't search through the entire hard drive looking for incriminating evidence.

Again, it is difficult to conceive a parallel in the physical world to how this software functions, but assume that George's banker's box is locked somehow. In fact, it's more like a safe that looks incredibly secure when it's sitting on the floor, but when the agents pick it up they find that the bottom is completely translucent. They are then able to see into the safe, and by shaking it the right way, they can expose and inspect each and every piece of paper. Consider whether such a search would be unconstitutional.

D. The Evolution of the Consent Search Doctrine

The Fourth Amendment to the United States Constitution provides that all citizens are free from "unreasonable searches and seizures."[65] The amendment also contains the warrant clause, which describes certain requirements a search warrant must meet in order to pass constitutional review.[66] That these requirements were spelled out in the text of the amendment led the Supreme Court to deem warrantless searches per se unreasonable.[67] Over time, a number of exceptions have been carved out of the general rule against warrantless searches. One exception to this rule is that a search conducted pursuant to an owner's voluntary consent is not unreasonable.[68] In *Zap v. United States*,[69] the Court upheld a warrantless search based on consent provided as a condition to obtain

---

64 Based on this Note's author's use of EnCase version 6.5.1.2. Screencaptures of EnCase version 6.5.1.2 are on file with this Note's author.

65 U.S. CONST. amend. IV.

66 *Id.*

67 Weeks v. United States, 232 U.S. 383, 393–94 (1914).

68 Zap v. United States, 328 U.S. 624, 626–28 (1946).

69 *Zap*, 328 U.S. at 626–28.

a government contract.[70] The landmark case *Schneckloth v. Bustamonte*[71] held that the non-owner driver of a car could verbally consent to a search of the car and that evidence retrieved from the trunk was admissible against him.[72]

Further development of the consent search doctrine has come from cases where the consenter was not an occupant of the property being searched. In *Stoner v. California*,[73] consent given by a hotel clerk did not effectively waive the guest's Fourth Amendment rights.[74] The *Stoner* Court was not convinced "that the night clerk had been authorized by the petitioner to permit the police to search the petitioner's room."[75] The Court was unwilling to allow "the rights protected by the Fourth Amendment . . . to be eroded by strained applications of the law of agency or by unrealistic doctrines of 'apparent authority.'"[76]

At issue in *United States v. Matlock*[77] was whether a consenter must have actual ownership of a home in order for her consent to be valid.[78] The *Matlock* Court expanded the consent search doctrine to include consent given by non-owners who "possess[] common authority" over the place to be searched.[79] The Court made clear that the authority to consent to a search does not stem from "the mere property interest" that the consenter may have, but instead is based on an assumption of risk that co-inhabitants make by virtue of sharing access to the common areas of a home.[80]

But the Fourth Circuit was quick to restrict the *Matlock* consent-search doctrine, and in *United States v. Block*[81] held that a mother did not have the authority to consent to a search of her twenty-three-year-old son's locked footlocker even though she

---

70 *Id.*
71 Schneckloth v. Bustamonte, 412 U.S. 218 (1973).
72 *Id.* at 248.
73 Stoner v. California, 376 U.S. 483 (1964).
74 *Id.* at 490.
75 *Id.* at 489.
76 *Id.* at 488.
77 United States v. Matlock, 415 U.S. 164 (1974).
78 *Id.* at 166–68.
79 *Id.* at 171.
80 *Id.* at 171 n.7.
81 United States v. Block, 590 F.2d 535 (4th Cir. 1978).

could consent to a search of his room.[82] The court had defined the scope of the mother's consent to include only the areas she had actual access to, and it was clearly discernable by the agents that she had no access to the locker.[83] A question still remained, however, as to the scope of consent when it is not clear to the agents whether the consenter had actual authority over the items to be searched.[84]

In the circuit courts, *Matlock* was interpreted to mean that consent by one co-inhabitant was binding on all co-inhabitants.[85] Post-*Matlock*, even a co-inhabitant with equal authority over a home could not effectively object to a search when another co-inhabitant had authorized it.[86] While this interpretation held for a majority of circuits, the Fourth Circuit held in *State v. Leach*[87] that *Matlock* applied only to co-inhabitants who were not present during the search, and thus a search conducted pursuant to the consent of one co-inhabitant, but without the consent of another present co-inhabitant, was unconstitutional.[88]

1. *Matlock* Revised: Objections Over Consent

Most recently, in *Georgia v. Randolph*,[89] the Court took on the competing interpretations of *Matlock* as it pertains to whether a co-inhabitant's consent can override another co-inhabitant's objection to a search.[90] The *Randolph* Court held that consent by one co-inhabitant can be invalidated by a present objecting co-

---

82 *Id.* at 541.

83 *Id.* at 540–41.

84 Jason M. Ferguson, *Article and Survey:* Randolph v. Georgia*: The Beginning of a New Era in Third-Party Consent Cases*, 31 NOVA L. REV. 605, 612–13 (2007).

85 *See id*. at 615–17.

86 *Id.* at 615 ("[C]ourts expanded the application of the *Matlock* standard to provide that a person with common authority over property may permit a warrantless search by law enforcement even if the defendant has equal authority over the property, is present at the time of the search, and specifically objects to the search.").

87 State v. Leach, 113 Wash. 2d 735 (Wash. 1989).

88 *Id.* at 736 ("At issue is the validity of a warrantless search where consent is obtained from a third party who possesses some control over the premises, but the defendant, who has superior control, is present at the time the search is conducted. We hold the police must obtain the consent of a cohabitant who is present and able to object in order to effect a valid warrantless search.").

89 Georgia v. Randolph, 547 U.S. 103 (2006).

90 *Id.* at 108–23.

inhabitant.[91] The Court took the opportunity presented in *Randolph* to clarify *Matlock* and what common authority actually means.[92] While recognizing that common authority is somewhat based on a property interest, the Court noted that the reasonableness of a search predicated on the consent of a co-inhabitant is rooted in notions of "widely shared social expectations."[93] The *Randolph* Court reasoned that, when co-inhabitants cannot agree on whether to consent to a search, the "resolution must come through voluntary accommodation, not by appeals to authority."[94] In reinforcing the right of one co-inhabitant to override another's consent to search, the Court was quick to caveat that the social expectations test need not be applied to cases of domestic violence or other exigent circumstances that would give the police the right to enter a home over the consent of one co-inhabitant.[95] Thus, in the modern era, whether a consent search is unreasonable as to a co-inhabitant is to be evaluated based on the inhabitants' social expectations and the law enforcement officer's reasonable inquiry into the validity of the consenter's access.

2. *Illinois v. Rodriguez*—Establishing Apparent Authority

In *Illinois v. Rodriguez*,[96] the Court clarified *Matlock's* other open question about a consenter's authority to allow police access to a home.[97] The Court expanded on *Matlock* by holding that police officers need only use reasonable care in determining whether a consenting individual possesses the requisite authority to sanction a search.[98]

In July of 1985, Mr. Rodriguez "was arrested in his apartment by law enforcement officers and charged with possession of illegal

---

91 *Id.* at 122–23.

92 *Id.* at 108–23.

93 *Id.* at 111.

94 *Id.* at 114.

95 *Id.* at 118–19; *see also* Renee E. Williams, Note, *Third Party Consent Searches after* Georgia v. Randolph*: Dueling Approaches to the Dueling Roommates*, 87 B.U. L. REV. 937, 949 (2007).

96 Illinois v. Rodriguez, 497 U.S. 177 (1990).

97 *See id.* at 179 (citing United States v. Matlock, 415 U.S. 164, 177 n. 14 (1974)) .

98 *Rodriguez*, 497 U.S. at 186; *see also* Georgetown Univ. Law Center, *Warrantless Searches and Seizures*, 36 GEO. L.J. ANN. REV. CRIM. PROC. 38, 78 n.250 (2007).

drugs."[99] The officers had been called "to the residence of Dorothy Jackson" to respond to an alleged assault perpetrated upon her daughter (Gail Fischer) by Mr. Rodriguez.[100] Throughout the subsequent police interview, Ms. Fischer led the police to believe that she shared an apartment with Mr. Rodriguez.[101] Fischer then led the police to the apartment and let them in with her key.[102] When the police entered, they found drug paraphernalia in plain view as well as containers of cocaine.[103] The police had never sought to obtain either a search warrant for Rodriguez's apartment or an arrest warrant for Rodriguez himself.[104]

At trial, Rodriguez argued that Fischer was not a resident of the apartment, citing the fact that she had moved out several weeks before.[105] The court agreed, holding that Fischer "was not a 'usual resident' but rather an 'infrequent visitor' at the apartment," and granted his motion to suppress all the evidence collected from the apartment.[106] The Appellate Court of Illinois affirmed the trial court's decision and the Supreme Court of Illinois declined to review the case.[107]

In its opinion, the Unites States Supreme Court reversed the trial court's decision, holding that the Fourth Amendment is not violated when law enforcement agents "reasonably (though erroneously) believe that the person who has consented to their entry is a resident of the premises . . . ."[108] Justice Scalia, writing for the Court, balanced the logic of *Stoner* against *Matlock* by noting first, that the question in cases of apparent authority is not whether an individual has waived her Fourth Amendment rights, but rather

---

99 *Rodriguez*, 497 U.S. at 179.

100 *Id.*

101 *Id.* ("During this conversation, Fischer several times referred to the apartment on South California as 'our' apartment, and said that she had clothes and furniture there. It is unclear whether she indicated that she currently lived at the apartment, or only that she used to live there.").

102 *Id.* at 180.

103 *Id.*

104 *Id.*

105 *Id.*

106 *Id.*

107 *Id.*

108 *Id.* at 186.

whether those rights were unreasonably violated, and second, that law enforcement officers may not assume that an individual possesses authority over a premises just because she says she does.[109] Instead, the officers' actions must comport with a more objective, reasonable man standard.[110]

3. Evaluating Consent: What is The Social Expectations Test?

The concept of individual privacy rights being established by social norms is fundamental to the evaluation of Fourth Amendment cases, though it has by no means defined them. As the Court noted in *Rakas v. Illinois*,[111] an individual's legitimate expectation of privacy "must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society."[112] Justice Harlan specifically noted in *Katz v. United States*[113] that the two-fold test for determining whether a particular intrusion offends the Fourth Amendment is based first on whether the individual had a subjective expectation of privacy, and second whether "society is prepared to recognize [it] as 'reasonable.'"[114]

The *Randolph* majority noted that, in the application of the Fourth Amendment to disputes over searches and seizures, "[t]he constant element . . . in the consent cases, then, is the great significance given to widely shared social expectations . . . ."[115] The Court posited that if an acquaintance were to show up on your doorstep and ask to come in, but your roommate stood in the doorway actively protesting, it would be, at the very least, a confusing situation for the acquaintance.[116] As a result, "no sensible person would go inside," unless some evidence of a life- or limb-threatening situation was apparent.[117] The resulting "customary

---

109 *Id.* at 187–88.
110 *Id.* at 188–89.
111 Rakas v. Illinois, 439 U.S. 128 (1978).
112 *Id.* at 143 n.12.
113 Katz v. United States, 389 U.S. 347 (1967).
114 *Id.* at 361 (Harlan, J., concurring).
115 Georgia v. Randolph, 547 U.S. at 103, 111 (2006).
116 *Id.* at 113–14.
117 *Id.* at 113.

social understanding" is that when a co-inhabitant is present, she may successfully bar the police from entering a home, but when she steps away from the property (provided the police have not coerced her absence), her privacy rests in her co-inhabitant's hands.[118]

Chief Justice Roberts's dissent in *Randolph* sharply criticized the majority's application of the social expectations test, as he believed it was "not a promising foundation on which to ground a constitutional rule . . . ."[119] Instead, Roberts argued that the Court ought to have evaluated this case based on whether Randolph possessed a "'*legitimate* expectation of *privacy*'" in the shared space.[120] That expectation, according to Roberts, does not exist for a co-inhabitant in a shared space.[121] Roberts argued that, while one might "trust" her co-inhabitant to not allow the police to search a shared space, it is not legitimate for her to expect that the trust will not be violated.[122] While there may be many social norms that people tend to adhere to with regard to shared secrets, the Constitution does not recognize them—it merely recognizes that privacy interest which protects shared information only "at the discretion of the confidant."[123] Seemingly in anticipation of future cases dealing with evidence stored on shared computers, Roberts specifically opined that, if a computer is shared between two co-inhabitants, they have ceded their expectations of privacy vis-à-vis each other.[124] His dissent did not, however, discuss this theory as applied to a computer that had been password-protected in the way that many home computers are.

---

[118] *Id.* at 120; *see also* Williams, *supra* note 95, at 949.

[119] *Randolph*, 547 U.S. at 130; *see also* Williams, *supra* note 95, at 950.

[120] *Randolph*, 547 U.S. at 131 (Roberts, C.J., dissenting) (first emphasis added) (quoting Rakas v. Illinois, 439 U.S. 128, 144 n.12 (1978)).

[121] *Id*. ("Our common social expectations may well be that the other person will not, in turn, share what we have shared with them with another—including the police—but that is the risk we take in sharing.").

[122] *Id.*

[123] *Id.*

[124] *Id.* ("If two roommates share a computer and one keeps pirated software on a shared drive, he might assume that his roommate will not inform the government. But that person has given up his privacy with respect to his roommate by saving the software on their shared computer.").

4. Exceeding the Scope of the Consent

The US Department of Justice maintains a cybercrime website that prominently features a manual which was created to aid law enforcement officers in conducting investigations that involve digital evidence and/or computer systems.[125] The manual extensively catalogues the legal landmines surrounding the acquisition and use of computer evidence in criminal matters.[126] The first section of the manual is devoted to "searching and seizing computers without a warrant" and includes an extensive discussion of the rules of consent searches as applied to computers.[127]

In *United States v. Jacobsen*,[128] the Supreme Court held that a third-party's consent to allow the police to look inside a package under the third-party's control was valid.[129] The *Jacobsen* Court, mindful of the difference between the third-party's search and the subsequent government action, clearly established the rule that government searches cannot exceed the scope of the initial private search.[130] Extending this precedent to a computer system, the DOJ Manual concludes that if a third-party has access to a computer, her consent can reasonably provide the basis for a search of the computer.[131] One caveat, however, is that under the *Jacobsen* rule, agents must often "inquire into third parties' rights of access" prior to initiating a search.[132] A second caveat is that agents must identify those areas to which the third-party has access and generally cannot search areas beyond the scope of common authority.[133]

---

125 DOJ MANUAL, *supra* note 13.

126 *Id.*

127 *Id.* at pt. (I).

128 United States v. Jacobsen, 466 U.S. 109 (1984).

129 *Id.* at 120–21.

130 *Id.* at 115–16 (citing Walter v. United States, 447 U.S. 649 (1980)).

131 DOJ MANUAL, *supra* note 13, at pt. (I)(C)(1)(b)(i) ("Agents may view what the third party may see without violating any reasonable expectation of privacy so long as they limit the search to the zone of the consenting third party's common authority.") (citation omitted); *see also Jacobsen*, 466 U.S. at 119–20.

132 DOJ MANUAL, *supra* note 13, at pt. (I)(C)(1)(b)(i).

133 *United States v. Block* held "that a mother could consent to a general search of her 23-year-old son's room, but could not consent to a search of a locked footlocker found in the room." DOJ MANUAL, *supra* note 13, at pt. (I)(C)(1)(b)(i) (citing United States v. Block, 590 F.2d 535, 541 (4th Cir. 1978)); *see also Jacobsen*, 466 U.S. at 115.

This doctrine was specifically extended by the Fourth Circuit to cover computer systems where multiple users have password-protected accounts.[134] In *Trulock v. Freeh*,[135] two people shared access to one computer system and, during the course of the interrogation, the police learned that they did not share their account passwords.[136] The *Trulock* court held that, because the investigating agents were aware that the party consenting to the search did not have access to the other party's files, the "consent . . . was insufficient to permit the search of Trulock's private computer files."[137] Rooting their analysis in an application of *United States v. Block*,[138] the circuit court determined that, even though the consenter in *Trulock* could legitimately "consent to a general search of the computer, her authority did not extend to Trulock's password-protected files."[139] The court did not address whether the consent would have been invalid had the investigating agents not discovered the password-protection scheme during their interview.

Another distinction that some defendants have raised is the difference between data stored on their computer and data stored on external media like floppy disks or CD-ROMs. These defendants then challenge searches on both fairness and constitutional grounds.[140] The courts have been unwilling to suppress external media recovered by the police pursuant to warrants that allow for the seizure of computer "equipment."[141] As the Tenth Circuit noted, there exists "no authority finding that computer disks and hard drives are closed containers somehow separate from the com-

---

134 Trulock v. Freeh, 275 F.3d 391 (4th Cir. 2001).

135 *Id.* at 403.

136 *Id.* at 398.

137 *Id.* at 399.

138 *Block*, 590 F.2d 535.

139 *Trulock*, 275 F.3d at 403; *see also Block*, 590 F.2d at 541.

140 *See, e.g.*, United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999) (holding that a second warrant for co-located computer disks was unnecessary when the police were authorized to search the computer); United States v. Simpson, 152 F.3d 1241, 1248 (10th Cir. 1998) (holding that external media were considered computer "equipment" and within the scope of the search warrant); United States v. Lacy, 119 F.3d 742, 746–47 (9th Cir. 1997) (a warrant allowing for a seizure of computer equipment was sufficient to allow for a seizure of disks).

141 *Simpson*, 152 F.3d at 1248.

puters themselves . . . ."[142] While *Simpson* was resolved in 1998, before Professor Kerr's article and the line of cases dealing with private data on shared computers, there is still generally no distinction between external media recovered along with a computer and the computer itself.[143]

E. Exceeding Authorization Through Technology

In addition to the legal issues surrounding consent searches, there are technological concerns that must be addressed in determining whether the police have exceeded their search authority. While they did not specifically address searches of computer systems, the Supreme Court in *Kyllo v. United States*[144] did discuss the use of specialized technology in criminal searches.[145] In *Kyllo*, the police used thermal imaging to discover "information regarding the interior of [Kyllo's] home."[146] The Court held that use of that technology constituted a search despite the fact that the officers never physically entered the home.[147] The Court's rationale was based in part on the fact that thermal imaging technology was "not in general public use," and in part because the intrusion by the officers was into Kyllo's home, a space deserving of the highest level of Fourth Amendment protection.[148]

The United States had argued that the thermal imager used in *Kyllo* was only able to pick up differences in temperature on the outside of the home's wall.[149] The Court found that the imager still technically searched inside the home, because "such a mechanical interpretation of the Fourth Amendment . . . would leave the homeowner at the mercy of advancing technology . . . that

---

142 *Id.*

143 *See, e.g.*, United States v. Grimett, 439 F.3d 1263, 1268–69 (10th Cir. 2006) ("[L]aw enforcement may not expand the scope of a search beyond its original justification . . . [and the warrant was to] search any computer media found therein."). *See generally* 2 WAYNE R. LAFAVE, SEARCH AND SEIZURE § 4.10 (4th ed. 2007).

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

145 *Id.* at 35–36.

146 *Id.* at 35 n.2.

147 *Id.* at 35–40.

148 *Id.* at 34.

149 *Id.* at 35.

could discern all human activity in the home."[150] That type of "intimate information," even if obtained without an officer ever entering the home itself, would clearly be considered within the scope of Fourth Amendment protection.[151] Even though there had been no physical intrusion into the home, the police technology invaded Kyllo's protected privacy interest, and thus the Court held that the officers had conducted a search.[152]

F. Consent Searches and Computer Files—Recent Case Law

1. *Trulock v. Freeh*

In the wake of *Randolph*, *Rodriguez*, and *Kyllo*, numerous courts have addressed the questions that arise when the police search a computer system using a software program like EnCase. In 2001, the Fourth Circuit heard a case which tested the boundaries of law enforcement activities vis-à-vis shared computers.[153] In *Trulock v. Freeh*,[154] the court heard about how FBI agents, investigating an alleged leak of classified information, questioned the plaintiff's girlfriend, Conrad, about a computer system that was shared by both of them.[155] During the questioning, the girlfriend reported that Trulock had his files stored under a password-protected user account to which she did not have the password.[156] While the ultimate issue in the case was not whether the search of the computer was unlawful, the *Trulock* court noted that "[a]lthough Conrad had authority to consent to a general search of the computer, her authority did not extend to Trulock's password-protected files."[157]

---

150 *Id.* at 35–36.

151 *Id.* at 34 ("[O]btaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search—at least where (as here) the technology in question is not in general public use." (quoting Silverman v. United States, 365 U.S. 505, 512 (1961))).

152 *Id.* at 34–35, 40.

153 Trulock v. Freeh, 275 F.3d 391 (4th Cir. 2001).

154 *Id.*

155 *Id.* at 398.

156 *Id.*

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

In determining whether Conrad's consent extended to Trulock's protected files, the Fourth Circuit made three interesting findings. First, the court analogized Trulock's password-protected area on the computer to a locked footlocker.[158] Second, the court found that Trulock's actions in protecting his files and withholding the password from Conrad established a reasonable expectation of privacy.[159] And finally, the court held that, because the law had been unsettled at the time the agents conducted the search and the agents could have reasonably believed that Conrad's consent was effective, they were entitled to immunity from the civil action against them.[160] However, *Trulock* left the law unsettled on the main issue of whether one user of a shared computer could ever consent to a search of the other user's password-protected files.[161]

2. *United States v. Buckner*

The Fourth Circuit, in *United States v. Buckner*,[162] tackled this issue six years later, upholding the legality of a search under the apparent authority doctrine.[163] The court sua sponte raised a separate argument regarding the methodology the police used to search

---

[158] *Id.* ("Trulock's password-protected files are analogous to the locked footlocker inside the bedroom.").

[159] *Id.* ("By using a password, Trulock affirmatively intended to exclude Conrad and others from his personal files. Moreover, because he concealed his password from Conrad, it cannot be said that Trulock assumed the risk that Conrad would permit others to search his files. Thus, Trulock had a reasonable expectation of privacy in the password-protected computer files and Conrad's authority to consent to the search did not extend to them.").

[160] *Id.* at 403–04.

[161] *Id.* at 404 ("[W]e are aware of no reported cases answering whether an individual has a reasonable expectation of privacy in password-protected files stored in a shared computer. Trulock, though conceding the absence of computer specific caselaw, urges us to recognize a clearly established right based upon *Block* and other similar cases. We decline to do this. Although cases involving computers are not [sui generis], the law of computers is fast evolving, and we are reluctant to recognize a retroactive right based on cases involving footlockers and other dissimilar objects.").

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

[163] *Id.* at 555 ("As long as the facts available to the officer at the moment . . . warrant a [person] of reasonable caution in the belief that the consenting party had authority, apparent authority to consent exists, and evidence seized or searched pursuant to that consent need not be suppressed." (internal quotation marks omitted) (quoting Terry v. Ohio, 392 U.S. 1, 21–22 (1968))).

Buckner's computer. In a footnote, the court stated that neither party argued "that the police officers *deliberately* used software that would avoid discovery of any existing passwords."[164] Since the issue was not contended, the court declined to rule on the merits, but noted in another footnote that the apparent authority doctrine would not likely extend to a situation where the police intentionally ignored a user's password protection.[165] Such a distinction, given the current state of technology, may sit on a very fine line, and as such the outcome of *Buckner* may have been quite different had Buckner argued that the technology allowed the police to bypass his password-protection.

3. *United States v. Andrus*

Most recently, the Tenth Circuit has confronted similar issues to those raised by *Trulock* and *Buckner*. In *United States v. Andrus*[166] the Tenth Circuit held, consistent with the Fourth Circuit opinions, that the apparent authority doctrine provided the basis for a search of a computer even when the consenter did not have actual authority to consent to the search.[167] In a divided decision, the *Andrus* court upheld a search of a computer that was available for use by three members of the Andrus family.[168] The consenter was the defendant's father and the search occurred when the defendant was not home.[169] The court relied heavily on the *Randolph* line of cases to establish the validity of the search based on the father's apparent authority.[170]

The *Andrus* court went further into the analysis and looked, like the *Trulock* court did, to analogize the computer to a physical container in order to determine the level of protection to afford it

---

164 *Id*. at 553 n.1.

165 *Id*. at 555 n.3 ("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 by the user.").

166 United States v. Andrus, 483 F.3d 711 (10th Cir. 2007), *reh'g en banc denied*, 499 F.3d 1162 (10th Cir. 2007).

167 *Id*. at 722.

168 *Id*. at 712, 721.

169 *Id*. at 713–14.

170 *Id*. at 716–17.

under the Fourth Amendment.[171] The court found, as courts before it had and as Orin Kerr has suggested, that the files stored on the computer were analogous to a footlocker or suitcase.[172] What the *Andrus* court then struggled with was how to deal with the fact that the defendant Andrus's files were password-protected such that Andrus's father could not normally access them.[173] This sticking point is the heart of the debate in the *Andrus* decision and in resolving the larger question of how to treat warrantless searches of modern computer systems.

It is worth noting that the *Andrus* majority did recognize a problem in allowing the agents to conduct a search of the computer when it became clear that Dr. Andrus did not have actual authority to consent to a search of his son's files.[174] At issue in the case, and in this Note, is whether law enforcement may, in a similar situation with a shared computer, continue to rely on a consenter's apparent authority at all when there are technological options that allow the agents to easily exceed the scope of consent.[175] If not, then the first step in any search of a shared computer system must be to determine the scope of the consenter's access, and no evidence should be analyzed or recovered prior to that determination being made.

II. BRIDGING THE GAP: APPLYING PHYSICAL CONSENT RULES TO DIGITAL MEDIA

When police officers conduct consent searches, they are limited to looking only at areas they reasonably believe are under the control of the consenter. But, as noted in the three recent cases that have dealt with consent searches of computer systems, there are two questions that must be answered to determine whether the

---

171 *Id.* at 718; *see also* Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir. 2001).

172 *Andrus*, 483 F.3d at 718; *see also* United States v. Buckner, 473 F.3d 551, 554 (4th Cir. 2007); *Trulock*, 275 F.3d at 403; United States v. Aaron, 33 F. App'x 180, 184 (6th Cir. 2006); Kerr, *supra* note 6, at 555.

173 *Andrus*, 483 F.3d at 718–19, 721.

174 *Id*. at 722.

175 *Id*. at 724 (McKay, J., dissenting).

police action is objectively reasonable.[176] The first is whether there has been a manifestation of the user's expectation of privacy.[177] That can be accomplished either overtly by the user encrypting or protecting her individual files or, as has been argued, could be assumed by the police due to the ubiquity of password protected user accounts and the ways that modern operating systems are configured. The second question is whether the expectation exhibited by the user is recognized by society as reasonable.[178] Beyond those two fundamental questions, *Kyllo* instructs courts to inquire whether the tools used by the police in their investigation are designed, and employed, to bypass the user account passwords that may have been put in place.[179]

A. Manifesting an Expectation of Privacy

1. Judge McKay's *Andrus* Dissent

The problem raised by the majority's opinion in *Andrus*, according to Judge McKay, is that the court failed to consider that the EnCase program used by the agents to search the Andrus computer was designed to find files irrespective of any password protections implemented at the user account level.[180] Two legal issues are at the core of this argument: (1) that the user has manifested his intent to keep the data private; and (2) whether the technology used by the police goes beyond the scope of the authorized search.[181] In his dissent, Judge McKay argued that EnCase is designed in a way that ignores the user-level password protections that many users

---

176 *See, e.g.*, Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

177 *Id.*

178 *Id*.

179 *See* United States v. Kyllo, 533 U.S. 27, 39 n.6 (2001) (noting that the Court can, and has in the past, made determinations about what type of activities are "routine"); DOJ MANUAL, *supra* note 13, at pt. (I)(B)(5) ("Use by the government of innovative technology not in general public use to obtain information stored on or transmitted through computers or networks may implicate this rule from *Kyllo* . . . . although courts have not yet defined the standard for determining whether a given technology meets this requirement.").

180 *Andrus*, 483 F.3d at 722 (McKay, J., dissenting).

181 *Id.* at 723.

implement.[182] But he tempered his argument with the recognition that sometimes the police cannot determine, through the technology, whether a consenter has the ability to access another user's files even though the accounts are password-protected.[183] Ultimately, Judge McKay argued that the police officers conducting this investigation should, at the very least, have inquired into the father's access to the computer prior to gaining his consent and conducting their search.[184]

The majority, on the other hand, interpreted the apparent authority doctrine as authorizing the police activity because the majority felt the police had enough evidence that the defendant's father was an authorized user of the computer.[185] But an authorized user of the computer may not be able to access every file on the computer just like a mother may not be able to access her son's locked footlocker.[186] The *Andrus* judges all considered this technical issue, but could not agree on the proper resolution.[187]

The *Randolph* Court was very clear in tying Fourth Amendment protections to an individual's reasonable expectation of privacy.[188] In the computer context, the courts have always been willing to protect individual files that a user has password protected or encrypted, but they have not gone as far as protecting data stored in an unprotected form, but in a folder only accessible by one user.[189] The *Andrus* court struggled with the issue of how a user's privacy is manifested with regard to those types of files.[190] The court seemed to recognize at least three different ways of ad-

---

182 *Id.*

183 *Id.* at 723 n.3 ("I recognize that the ability of users to program automatic log-ins and the capability of operating systems to 'memorize' passwords poses potential problems, since these only create the appearance of a restriction without actually blocking access.").

184 *Id.* at 724 ("The burden on law enforcement to identify ownership of the computer was minimal. A simple question or two would have sufficed.").

185 *Id.* at 720–21.

186 *Id.* at 717–18; United States v. Block, 590 F.2d 535, 541 (4th Cir. 1978).

187 *Compare Andrus*, 483 F.3d at 720, *with id.* at 724–25 (McKay, J., dissenting).

188 Georgia v. Randolph, 547 U.S. 103, 111 (2006).

189 *See* Trulock v. Freeh, 275 F.3d 391 (4th Cir. 2001); Steven E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 530–35 (2005) (arguing against Orin Kerr's notion that encryption itself does not create a reasonable expectation of privacy).

190 *See Andrus*, 483 F.3d at 718–19.

dressing this issue: (1) the police can freely search the computer relying on the apparent authority of the consenter so long as the computer is located in a common area in the home;[191] (2) the police can be required to inquire about the level of access the consenter has before conducting their search;[192] and (3) the police can use technological measures to determine whether a user has manifested a desire to protect her files.[193] The crux of the first part of this debate, then, is what steps must users take to clearly manifest their intention to keep their data private?

2. Mandatory Inquiry into Consenter's Access

The apparent authority doctrine requires only that a reviewing court look to whether the police officers had a reasonable belief that the consenter had access to the area they have asked to search.[194] In a situation where a computer is located in a common area in a home and the consenter is a family member who lives in the home, the police might reasonably believe that the consenter has access to the computer, but a more searching inquiry may be required.[195] If the police were to ignore information that would make a reasonable person believe the consenter lacked actual authority to grant consent the search would be in clear violation of the reasonable inquiry rule set forward by *Rodriguez*.[196] The objective standard by which police action should be judged in cases involving consent searches of computer equipment is very hard to establish because of the inherent ambiguities pointed out by the *Andrus* majority.[197] However, the Court clearly established in *Rodriguez* that it is precisely when the situation is ambiguous that the obligation to inquire attaches.[198]

---

191 *See id.* at 719.

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

193 *Cf. id.* at 723–24 (noting that the agents discovered the password protection after they began analyzing the computer with forensic investigation software).

194 *See* Illinois v. Rodriguez, 497 U.S. 177, 183 (1990).

195 *See Andrus*, 483 F.3d at 725 (McKay, J., dissenting) (citing *Rodriguez*, 497 U.S. at 188).

196 *See Rodriguez*, 497 U.S. at 188–89.

197 *See Andrus*, 483 F.3d at 717–22.

198 *Id.* at 724–25 (McKay, J., dissenting); *see also Rodriguez*, 497 U.S. at 188.

If, as the *Andrus* majority noted, the use of password-protected accounts poses difficulties for police in determining where the borders of one user's consent ought to be drawn, then Judge McKay is right, and the police officers should be required to, at the very least, ask about the consenter's level of access to the computer. Such an inquiry would be a quick and easy way for the police to discover whether the user had manifested an intent to keep her data private. Of course, the Court's caveat about lying consenters must remain in place if the police are only required to ask about the consenter's level of access, but technology could make even that inquiry insufficient.[199]

3. Is Password Use Ubiquitous?

Mr. Andrus argued that the police should have known that the shared computer would have multiple password-protected accounts on it, but the court noted that the defendant never offered any evidence that would "demonstrate a high incidence of password protection among home computer users."[200] But Judge McKay questioned the majority, asking what evidence the defendant could have introduced that would constitute "sufficient proof of the prevalence of password protection . . . ."[201] If the agents were aware that most users choose to employ password protection on their computers, the *Andrus* majority noted, then perhaps the agents would have been required to inquire about the consenter's access, but the majority found no evidence to suggest the police could have reasonably suspected that such protections were enabled.[202] The majority ignored, however, that the agents investigating Mr. Trulock, approximately six years prior to the investigation into Mr. Andrus's activities, had asked Conrad about passwords during their ques-

---

[199] The *Rodriguez* Court acknowledged that police could be misled by consenters, purposefully or not, and since the legal inquiry is the objective one of whether a reasonable person in the same position would have believed the consenter had authority to allow the search, the reviewing court should not hold the police liable for the consenter's deception. *Rodriguez*, 497 U.S. at 186–88.

[200] *Andrus*, 483 F.3d at 721.

[201] *Id.* at 723 (McKay, J., dissenting).

[202] *Id.* at 721–22, 722 n.8.

tioning.[203] The majority seemed to contradict itself by noting in one case 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," but then failing to apply that analysis to the agents' conduct in the second case.[204] This contradiction occurred because the majority considered the computer a self-contained physical device, not a data storage system which should be treated as multiple logical devices.[205]

B. EnCase, Kyllo, *and Unreasonable Searches*

The *Andrus* court's analysis of the difficulties inherent in determining whether a user has enabled password protection for his account can be exacerbated by the realities of the physical-digital distinction. As stated earlier in this Note, users can enable passwords on their accounts and effectively prevent other users of the system from accessing their files.[206] But those protections are abrogated when someone with physical access to the computer uses a program that looks directly at the data on the hard drive and bypasses the operating system's security features. The *Buckner* Court specifically noted, in upholding the search allowed by Buckner's girlfriend, that if the officers intentionally ignored or used techniques that would avoid detecting password protections they would not be able to rely on the apparent authority doctrine to justify the search.[207]

While courts have been divided about how strictly to apply the Fourth Amendment's warrant particularity requirement to searches of computer hard drives, investigators are advised to specify, in the warrant, the types of files they are seeking.[208] Should the investi-

---

[203] Trulock v. Freeh, 275 F.3d 391, 398 (4th Cir. 2001).

[204] *Andrus*, 483 F.3d at 718.

[205] *See* Kerr, *supra* note 6, at 438–40 (discussing the differences between physical searches of homes and searches of data on hard drives).

[206] *See supra* Part I.A.

[207] United States v. Buckner, 473 F.3d 551, 555 n.3 (4th Cir. 2007).

[208] *See* United States v. Carey, 172 F.3d 1268, 1274 (10th Cir. 1999) (holding that agents exceeded the scope of a warranted search when they stopped looking for evidence of drug-related crimes and began looking for child pornography). *But see* United States v.

gator inadvertently discover evidence of a type not specified in the warrant, she should seek additional authority before searching for further evidence of that type.[209] In addition, a debate exists between the Fifth and Tenth Circuits as to whether investigators exceed the scope of consent when they search different areas of a hard drive than those they initially asked to see.[210] Whether a search is improper because of the inherent nature of the tool used to conduct it is another inquiry altogether.

The *Kyllo* Court was concerned with the application of technology that allowed the police to do things that the general public could not do, essentially looking through a wall.[211] To make clear how EnCase could be inherently violative of the Fourth Amendment, consider the following two hypotheticals, similar to *Kyllo* and George Costanza's situation from this Note's introduction.

Assume that Kozmo Kramer was growing marijuana in a closet in the basement of his home and that his girlfriend, Elaine Benes, only entered the basement once a week to do laundry. Mr. Kramer keeps the door to his grow-room locked with a padlock to which only he has the key. He has told his girlfriend that he keeps the door locked because there are very valuable family heirlooms in there, and he only has one key to the lock, which he keeps in his pocket at all times. Because Mr. Kramer is incredibly careful to mask the odor of the marijuana plants, Ms. Benes is totally oblivious to Mr. Kramer's illicit activities until one day, when Mr. Kramer is not at home, the DEA knocks on the door. The DEA agents inform Ms. Benes that they believe her boyfriend has an illegal marijuana farm in the house and they would like to take a

---

Hudspeth, 459 F.3d 922, 926–28 (8th Cir. 2006) (upholding a warranted search where the agents found pornography while conducting a search for business records), *vacated en banc, then reinstated in part*, 518 F.3d 954 (8th Cir. 2008).

209 *See* United States v. Gray, 78 F. Supp. 2d 524, 530–31 (E.D. Va. 1999) (upholding a search where officers obtained a second warrant before searching for child pornography when the warrant had been drafted to allow searching for evidence of computer hacking).

210 *Compare Carey*, 172 F.3d at 1274, *with* United States v. Slanina, 283 F.3d 670, 680 (5th Cir. 2002) (holding that once a search of a portion of the defendant's computer has been justified, the defendant has no reasonable expectation of privacy in the data on the computer). *But see* Kerr, *supra* note 6, at 576–82 (arguing that a new approach to the plain view doctrine is necessary for computer evidence).

211 *See supra* Part I.E.

look around. Ms. Benes is shocked to hear that her boyfriend would be involved in something like that, and so she gives them permission to search the home.

Obviously, when the agents reach the locked door in the basement, they will see the padlock. Even if, hypothetically, there was no overt sign of a lock, when they tried to open the door the agents would find that they could not access the room. But, and this is where Orin Kerr's distinctions between digital and physical searches are extremely relevant, if the police chose to, instead of physically searching the house, use a thermal imager to scan for rooms with heat signatures matching marijuana grow lights, would the discovery of the locked room in the basement violate Mr. Kramer's Fourth Amendment rights?

On one hand, Ms. Benes consented to a search of the home, and the police may have even informed her that they would be using thermal imaging in the course of that search. On the other hand, however, without the aid of that technology, the police would never have been able to obtain access to or discover that room, and it is clear that Ms. Benes has no right to consent to a search of it.[212]

Now imagine that the shared home computer is what the agents want to examine. If Mr. Kramer had encrypted his data and locked it away from his girlfriend, any court would likely rule that the agents cannot break the lock.[213] But if he chose to secure his private data by locking the computer with different password-protected accounts so that his girlfriend could log on to occasionally play solitaire and his secret activities would remain that way, under the *Andrus* ruling, the same protections would not apply.[214]

---

[212] *See* United States v. Block, 590 F.2d 535, 541 (4th Cir. 1978). Note, however, that if the two were married, the consent that the wife gives to search the house could arguably be extended to allow access to all the rooms, even the ones where the husband has forbidden the wife to go. *See, e.g.*, Stein v. United States, 166 F.2d 851, 855 (9th Cir. 1948) (noting that even when a spouse is no longer residing in the marital home, "the right of [defendant's wife] to enter the house cannot be seriously questioned . . ."). Such a situation is beyond the scope of this Note.

[213] *See* United States v. Andrus, 483 F.3d 711, 717 (10th Cir. 2007), *reh'g en banc denied*, 499 F.3d 1162 (10th Cir. 2007).

[214] *See id.* at 716.

In that situation, the use of EnCase is almost exactly analogous to the use of the thermal imager, because the agents conducting the search are using software that was specifically designed to search through a hard drive without considering the locks put in place at the user-account level.[215]

Judge McKay's dissent in *Andrus* made clear that he thought EnCase was a problematic tool in the context of a consent search.[216] In the subsequent decision where the Tenth Circuit denied rehearing in the case, the court noted that the only valid issue raised in the petition for rehearing was whether the defendant's father's consent was sufficient and the argument "premised on *Kyllo v. United States* . . . was made for the first time in [the] petition for rehearing and was . . . therefore forfeited."[217]

III. FORENSIC INVESTIGATORS MUST ATTEMPT TO DISCOVER PASSWORD PROTECTED ACCOUNTS PRIOR TO CONDUCTING CONSENT SEARCHES

If, during the course of a forensic investigation on a computer hard drive acquired pursuant to a consent search, the investigator realizes that there are password protections enabled for one of the accounts, the investigator should stop looking at the data and attempt to confirm that the consenter had access to the files before continuing the search.[218] The process for determining whether accounts are password protected using EnCase is trivial. Running the script that EnCase uses to display the account information takes mere seconds of investigator time and can be run after the seizure but before any data are exposed. Since *Rodriguez* requires that the police at least inquire about the authority of the consenter,[219] it would make sense that if they could definitively ascertain whether the computer had password protection prior to beginning their

---

215 *See id.* at 723 (McKay, J., dissenting).

216 *Id*.

217 United States v. Andrus (*Andrus II*), 499 F.3d 1162, 1163 (10th Cir. 2007) (denying rehearing en banc).

218 *See Andrus*, 483 F.3d at 724 (McKay, J., dissenting) (citing United States v. Buckner, 473 F.3d 551, 555 & n.3 (4th Cir. 2007)).

219 *See* Illinois v. Rodriguez, 497 U.S. 177, 188–89 (1990).

analysis, they should be required to do so.[220] This method does not eliminate all of the problems that simple inquiry would have (e.g., consenters can still lie about their access rights to the computer), but it does make certain that the police have done all they reasonably can do before beginning their search. It is irrelevant, then, whether or not password use is commonplace among users of home computers, because the investigator can tell whether the specific computer about to be analyzed is protected.

A determination that the computer has some password-protected accounts does not mean that a search of the computer would be unlawful. It may be the case that the password-protected account is shared between multiple users. It is possible that, as Judge McKay pointed out in *Andrus*, the computer is configured with a password-protected account that automatically logs in when the computer is powered on.[221] Further, the consenter's account may be an administrator account and might be able to access all of the data on the hard drive. In situations where the consenter's level of access cannot be determined by the technology alone, the police should conduct an inquiry before continuing the investigation. A multi-user computer system presents an inherent ambiguity in whether the consenter has access to all of the data on the hard drive, and when that ambiguity exists the police must conduct a reasonable inquiry to determine what the consenter's level of access is.

The use of EnCase and software like it poses a very significant problem in the context of consent searches. By its very nature, the software ignores certain security features that the computer operating system provides. Users who have chosen to protect their data from the co-users by enabling password-protected accounts would likely expect that their co-users cannot access their data. They possess an expectation of privacy similar to the expectation one might have if she kept her valuables in a locked safe. What many users do not know, however, is that cracking that safe is as simple as looking at it from a different angle. But it would be a critical er-

---

[220] Even if the software provided imperfect results, it would at least provide a basis for the investigator to question the scope of the consenter's access.

[221] *See Andrus*, 483 F.3d at 723 n.3 (McKay, J., dissenting).

ror for a court to hold that a search using technology like EnCase is permissible when it specifically bypasses those security features. Perhaps users should know that their data are not as secure as they might think, but that argument could also be used to legitimize the search in *Kyllo*, since it is conceivable that people are aware that thermal imaging technology exists. Mr. Kyllo could have put his grow-lamps in a room built out of material which dissipated the heat and made thermal imaging ineffective, but to require that kind of manifestation of an expectation of privacy goes well beyond the constitutional protections from unreasonable searches. The courts should not sanction the use of technologies that evade reasonable security protections no matter how weak they are.

A. The Future

Heavy computer users know that even the largest internal hard drive can quickly be filled with data. Users have been copying their data to external storage devices for decades as a means of preserving their data.[222] Now, however, zip disks are slow and expensive, so users are saving their back-up data on external hard drives.[223] One of the technologies to recently jump from the office to the home computing environment is the network hard drive.[224] These are standalone data storage devices which are accessed via a user's home network.[225] Users of these network drives can choose to configure multiple user accounts just like they can on their computers.[226]

---

[222] There are many ways a computer user can backup her data. Users generally copy data to an external disk which, in the past, would have been a floppy disk. *See* IBM Archives: 20th Century Disk Storage Chronology, http://www-03.ibm.com/ibm/history/exhibits/storage/storage_chrono20.html (last visited Oct. 28, 2008); Wikipedia—Floppy Disk, http://en.wikipedia.org/wiki/Floppy_disk (last visited Aug. 25, 2008) (historical perspective on the development of the external disk dating back to the 1970s).

[223] *See, e.g.*, Maxtor OneTouch 4 Plus, http://www.maxtor.com/en/external-drives/external-hard-drive/index.html (last visited Oct. 28, 2008).

[224] *See* Western Digital—My Book World Edition 1 TB Hard Drives, http://www.wdc.com/en/products/Products.asp?DriveID=347 (last visited Oct. 28, 2008).

[225] *Id.*

[226] WESTERN DIGITAL, MY BOOK WORLD EDITION USER MANUAL 35–38 (2007), *available at* http://www.wdc.com/en/library/usb/2779-701026.pdf.

Unlike a stand-alone computer, however, the forensic technology may not be able to easily discover whether there are passwords in place which restrict access to certain files. As well, a co-inhabitant may not be aware that another co-inhabitant has installed such a device on the network. The issue that courts may soon need to resolve is whether to treat these hard drives like other external media (e.g., CD-ROMs, Zip Disks, etc.), or computers themselves.

By treating these network drives like other external media, the court would sanction police seizure and search of the data on them, just as in *Andrus*, and the only way a user could protect herself from such a search would be to password-protect or encrypt the individual files. To require encryption in the case of a storage mechanism that is password-protected, based on the inquiry requirement imposed in *Trulock*,[227] would be an unreasonable burden on users.

As storage devices become more sophisticated and integrate certain functions normally reserved only to stand-alone computers, the line between what is external media and what is a computer will continue to be blurred. Certainly, courts should approach these new technologies just as they approach any new technology: by applying the rules of law from the most analogous situations to the new one the court faces.[228] As the courts encounter these new storage technologies that allow users to secure their data from other users of the same device, they should construe the restrictions on law enforcement activity as narrowly as possible in order to protect an individual's reasonable expectation of privacy.[229]

---

[227] *See* Trulock v. Freeh, 275 F.3d 391, 402–03 (4th Cir. 2001) (citing Stoner v. California, 376 U.S. 483 (1964)).

[228] *See generally* Katz v. United States, 389 U.S. 347 (1967).

[229] *Id.* at 361 (Harlan, J., concurring) ("My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").