PROPPING UP THE ILLUSION OF COMPUTER PRIVACY IN *UNITED STATES V. BURGESS*

INTRODUCTION

Imagine that, like many Americans, you bring your laptop to and from the office every day. On it you have sensitive work information, perhaps personal photos and correspondences, and your browsing history. Imagine also that on your drive to work you get pulled over and the police have probable cause to search your vehicle. Can they flip open your laptop and begin browsing your work files? Your personal files? Your browsing history? Can they restore your deleted files and search those?

Now imagine they are looking for evidence of drug trafficking. Is there a limit to the types of files they may open? Can they open only spreadsheets or files with suspicious names, such as "heroinproceeds.xls?" Can they look at your personal photos, or your browsing history? And, if they find evidence of a different crime, can they use it against you?

Those are some of the questions faced by David Burgess and the authorities that searched two hard drives found in his motor home during a traffic stop. When the Tenth Circuit Court of Appeals reviewed Burgess's case, it attempted to answer two specific questions: First, do computers qualify as containers, along with all the implications to a search that conclusion brings; second, if computers are containers, do any discernible concepts limit law enforcement access to personal computer files?

Part I of this Comment summarizes the Tenth Circuit's analysis of these issues in *United States v. Burgess*,[1] the court's most recent foray into the world of computer privacy. Part II examines the implications of treating a computer like a container, concluding that in several instances such a treatment will result in a greater number of searches of computers. Part III considers whether other Fourth Amendment doctrines will increase or decrease the privacy right associated with a computer and its contents. In Part IV, this Comment examines the difficulties involved in limiting the scope of computer searches. Finally, Part V concludes that the privacy protections applied in *Burgess* were wholly illusory, and argues that the court should have either rejected additional safeguards for computer privacy, or applied real—not illusory—computer privacy pro-

[1] 576 F.3d 1078 (10th Cir. 2009).

tections by following the approach taken by the Ninth Circuit in *United States v. Comprehensive Drug Testing, Inc.*[2]

I. *United States v. Burgess*

A. Facts

At a restaurant parking lot in Evanston, Wyoming, State Trooper Matt Arnell spotted a motor home known to be associated with the Hell's Angels motorcycle club bearing Nevada license plates and towing a trailer with expired Wyoming license plates.[3] Arnell followed the vehicle onto Interstate 80; after calling the dispatcher to request the assistance of a canine drug unit, he pulled over the motor home in order to cite the owner for the expired plates.[4] As the driver, Shayne Waldron, exited the motor home, Arnell smelled the odor of burnt marijuana emanating from the vehicle.[5] While Arnell spoke with Waldron, David Burgess—the owner of the motor home—joined the conversation.[6] Before Arnell finished writing the citation, Deputy David Homar arrived with his police dog, Blitz, who alerted to the motor home's doors.[7]

Arnell informed Burgess of his intent to search the motor home.[8] Burgess requested that Arnell obtain a warrant.[9] Based on the marijuana odor and Blitz's alert, however, Arnell proceeded to search the motor home without a warrant.[10] Arnell found marijuana, a pipe, and fourteen grams of cocaine in the motor home.[11] Burgess admitted that the marijuana belonged to him.[12] Arnell continued the search, locating a laptop computer and a Seagate hard drive.[13] Arnell seized the vehicle, which was towed to a Wyoming Department of Transportation facility for additional inspection.[14]

Arnell and Agent Russell Schmidt of the Green River police department offered a sworn affidavit and requested a warrant to search the hard drives.[15] Agent Schmidt stated in the affidavit that drug traffickers often keep photos of drugs and their co-conspirators in their vehicles.[16] The county judge approved the warrant, authorizing a search of the hard

[2] 579 F.3d 989 (9th Cir. 2009) (en banc).

[3] *Burgess*, 576 F.3d at 1082.

[4] *Id.*

[5] *Id.*

[6] *Id.*

[7] *Id.* According to the court, Blitz had never falsely signaled the presence of drugs. *Id.*

[8] *Id.*

[9] *Id.*

[10] *Id.*

[11] *Id.*

[12] *Id.* at 1083.

[13] *Id.* The first search took less than thirty minutes. *Id.*

[14] *Id.*

[15] *Id.*

[16] *Id.* Agent Hughes described these as "trophy photos." *Id.* at 1084 (defining "trophy photos" as "pictures of 'a person holding the controlled substance in front of a stack of money'").

drives for records, "pay-owe sheets," and "items of personal property which would tend to show conspiracy to sell drugs."[17]

Agent Scott Hughes of the Internet Crimes Against Children Division was assigned to search the seized hard drives.[18] Following protocol, Hughes used the "EnCase" computer program to duplicate the contents of the hard drives seized from Burgess's motor home.[19] The EnCase program allows an investigator to preview files as they are being copied.[20] The previewed files are displayed in a "gallery view" at a reduced size, many to a page.[21] Hughes used this feature to look for photos of controlled substances while the drive was being copied.[22] Hughes had viewed 200 to 300 digital images while the files were transferring when he discovered an image depicting child sexual exploitation.[23] Pursuant to a DCI staff attorney's instructions, Hughes then stopped his search and requested a new warrant authorizing a search for evidence of child sexual exploitation.[24] Searching under the auspices of the new warrant, Hughes found numerous images of child pornography on both the hard drives seized from Burgess's motor home.[25]

A grand jury indicted Burgess under 18 U.S.C. § 2252A(a)(1), which prohibits the knowing transportation of child pornography across state lines, and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2), which prohibits the knowing possession of child pornography transported in interstate commerce.[26] Prior to trial, Burgess moved to suppress the evidence found on the hard drive that was the basis for his indictment on both counts.[27] Burgess claimed the initial search of the hard drive, which sought to uncover evidence of drug trafficking, violated the Fourth

[17] *Id.* at 1083. The warrant described:

> "The property and premises of a white, 1999, Freightliner Motorhome . . . [for] certain property and evidence to show the transportation and delivery of controlled substances, which may include but not limit[ed] to, cash, or proceeds from the sale of controlled substances, Marijuana, Cocaine, Methamphetamine, or other illegal controlled substances, along with associated paraphernalia to include but not limited to pipes, bongs, syringes, packaging material, computer records, scales, laboratory dishes, flasks, beakers, tubes, pie tins, electrical timers, containers to be used for storing, manufacturing and selling, chemicals used in the creation of illegal narcotics as well as their diluting agents, items of personal property which would tend to show conspiracy to sell drugs, including pay-owe sheets, address books, rolodexes, pagers, firearms and monies."

Id. (alterations in original).

[18] *Id.* The warrant allowed the agents to search Burgess's laptop, the Seagate external hard drive, and a second hard drive manufactured by Maxtor. *Id.* However, the warrant's scope was limited to searching for evidence related to controlled substances. *Id.* Agent Hughes was instructed by a DCI staff attorney to obtain a new warrant should he find evidence of other crimes. *Id.*

[19] *Id.* at 1083–84.

[20] *Id.* at 1084.

[21] *Id.*

[22] *Id.*

[23] *Id.*

[24] *Id.* at 1083–84.

[25] *Id.* at 1084. Although he stopped counting at 1,300 images, Hughes estimated the total number of images of child pornography contained on the two hard drives was over 70,000. *Id.*

[26] *Id.*

[27] *Id.* Burgess filed additional motions outside the scope of this Comment. *Id.*

Amendment requirement that search warrants describe items sought by the government with sufficient particularity.[28] The government countered by asserting that even if the warrant was deficient, the search was still permissible under the automobile exception.[29] Rather than rely solely on the automobile exception to uphold the search, the United States District Court for the District of Wyoming found that the warrant contained sufficient particularity with respect to the items to be seized.[30] A jury convicted Burgess on both counts, and he appealed the denial of his motion to suppress.[31]

B. The Tenth Circuit's Opinion

Examining Burgess's case, the Tenth Circuit considered two methods of applying Fourth Amendment protections to computers. First, the court considered whether a computer is a container and therefore subject to search under the automobile exception.[32] Second, the court considered whether it was possible to fashion a rule that would adequately limit the scope of computer searches without precluding such searches altogether. Although the Tenth Circuit expressed concern about the potential abuse of computer searches, it ultimately failed to devise a rule that would protect citizens from "file-by-file" rummaging without significantly interfering with legitimate law enforcement interests.

1. Are computers containers?

Under the automobile exception announced in *Carroll v. United States*,[33] an officer may perform a warrantless search of a vehicle, provided probable cause exists.[34] In *California v. Acevedo*,[35] the Supreme Court held that the automobile exception applies uniformly to the interior of a vehicle, *including any containers that are present*.[36] Because the Tenth Circuit had previously analogized a computer to a suitcase,[37] it would be a small step for the court to hold that the automobile exception allows officers to search a laptop computer without a warrant when the

[28] *Id.*; *see also* Defendant-Appellant's Reply Brief at 5, *Burgess*, 576 F.3d 1078 (No. 08-8053), 2009 WL 1258555 ("The Fourth Amendment requires that a search warrant describe the things to be seized with sufficient particularity to prevent a general exploratory rummaging in a person's belongings." (internal quotation marks omitted) (quoting United States v. Campos, 221 F.3d 1143, 1147 (10th Cir. 2000))). *See generally* United States v. Hargus, 128 F.3d 1358, 1362 (10th Cir. 1997) ("A warrant's description of things to be seized is sufficiently particular if it allows the searcher to reasonably ascertain and identify the things authorized to be seized.").

[29] *Burgess*, 576 F.3d at 1084.

[30] *Id.*

[31] *Id.* at 1086–87. Burgess' other arguments on appeal are outside the scope of this Comment.

[32] *Id.* at 1087–88.

[33] 267 U.S. 132 (1925).

[34] *Id.* at 155–56.

[35] 500 U.S. 565 (1991).

[36] *See id.* at 580.

[37] *See* United States v. Andrus, 483 F.3d 711, 718 (10th Cir. 2007), *cert. denied sub nom.* Andrus v. United States, 552 U.S. 1297 (2008).

computer is found pursuant to a vehicle search supported by probable cause.[38] The *Burgess* court reinforced this possibility by referencing the language of *Acevedo*, which "interpret[ed] *Carroll* as providing one rule to govern all automobile searches."[39] This "one rule" language could foreclose the possibility of treating a computer differently than a container, if the Tenth Circuit correctly interpreted *Acevedo* as compelling the equal treatment of all objects capable of containing evidence in an automobile. As the court stated, "Nothing in *Acevedo* suggests [a computer search] . . . would be impermissible without a warrant . . . ."[40]

The court also discussed an alternative[41] to treating a computer as a container: treating it as a "virtual home."[42] Because computers are capable of storing vast amounts of personal information, they may deserve the enhanced Fourth Amendment protections the Supreme Court has so far reserved only for homes.[43] Indeed, the *Burgess* court cited a Tenth Circuit precedent cautioning that "the sheer range and volume of personal information the computer may contain" argues for treating a computer differently than a simple container.[44]

The Tenth Circuit found no case law that directly addressed the issue, and ultimately declined to resolve it.[45] The court skirted the "one rule" language presented by *Acevedo*, stating the truism, "[S]eemingly well-settled matters are subject to change,"[46] and referencing the Supreme Court's recent change to Fourth Amendment automobile exception jurisprudence in *Arizona v. Gant*.[47] The Tenth Circuit explained:

[38] *Burgess*, 576 F.3d at 1087–88.

[39] *Id.* at 1089 (internal quotation marks omitted) (quoting *Acevedo*, 500 U.S. at 579).

[40] *Id.* at 1090.

[41] The court also implies a third way of treating a laptop, suggesting that its *United States v. Carey* decision created different rules for seizure than for searching a laptop. *See id.*; United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999). Under *Carey*, a laptop may be seized and secured while a warrant is obtained. 172 F.3d at 1275. This begs a comparison with the Supreme Court's treatment of automobiles. In *Chambers v. Maroney*, the Court suggested that a vehicle could either be searched pursuant to the automobile exception, or could be seized and secured until a warrant is issued. 399 U.S. 42, 52 (1970). Yet in that very same case, the Court upheld a warrantless search of a vehicle in custody. *Id.* This treatment also raises the question of what level of suspicion should be required of an officer seizing a digital storage device. With the prevalence of laptops, cell phones, iPods and Blackberry devices, the likelihood of a person encountering law enforcement having such a device in their vehicle is high. A low standard for seizure of these devices may incentivize law enforcement to seize them routinely without individualized suspicion. On the other hand, a high standard of seizure may not be reconcilable with *Acevedo*'s ruling that no individualized suspicion is required to search containers within a permissibly searched automobile.

[42] *Burgess*, 576 F.3d at 1088.

[43] *Id.* at 1088–89.

[44] *Id.* at 1088 (citing United States v. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009)).

[45] *Id.* ("[T]he parties have cited no case law which either allows or prohibits computer equipment searches under the automobile exception and our research has failed to uncover such authority.").

[46] *Id.* at 1090.

[47] *Id.* (citing Arizona v. Gant, 129 S. Ct. 1710, 1722 (2009); New York v. Belton, 453 U.S. 454, 460 (1981)).

> In spite of clear language in *Acevedo*, one might speculate whether the Supreme Court would treat laptop computers, hard drives, flash drives or even cell phones as it has a briefcase or give those types of devices preferred status because of their unique ability to hold vast amounts of diverse personal information.[48]

Despite its extensive discussion of the manner of application of the Fourth Amendment to computers found during valid automobile searches, the *Burgess* court avoided the issue by simply affirming the District Court's holding that the warrant issued to search Burgess's motor home was valid.[49]

2. Scope of a computer search

Although the *Burgess* court failed to grant preferential Fourth Amendment protections to laptop computers in automobiles, it nevertheless considered ways to limit the scope of permissive computer searches.[50] Specifically, the court asked whether there was anything Agent Hughes was compelled to do to protect Burgess's privacy rights associated with his computers. The court concluded, however, that there is no good way to limit the scope of a computer search, and that such searches will always amount to general searches of the computer's contents. "[I]n the end," the court explained, "there may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders, and that is true whether the search is of computer files or physical files."[51]

At first blush, this holding appears to run contrary to two prior decisions issued by the court. First, in *United States v. Carey*,[52] the court said in a dictum that computer searches should be limited to the information specified in the warrant through methods such as "observing files types[53] and titles listed on the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory."[54] Second, in *United States v. Walser*,[55] the Tenth Circuit held that a computer search must be conducted in a manner that "avoids searching files of types not identified in the warrant."[56]

[48] *Id.*

[49] *See id.* at 1088, 1091. Because the laptop in an *Acevedo* search issue was presented by the Government as an alternative method of finding the search of Burgess's computers valid, the upholding of the warrant's validity rendered that issue moot. *See id.* at 1091–92.

[50] *Id.* at 1092–93.

[51] *Id.* at 1094.

[52] 172 F.3d 1268 (10th Cir. 1999).

[53] File types are often identified by a string of alpha-numeric characters appended to the file name known as "file name extensions." *See, e.g.*, *Burgess*, 576 F.3d at 1093 & n.16.

[54] *Carey*, 172 F.3d at 1276.

[55] 275 F.3d 981 (10th Cir. 2001).

[56] *Id.* at 986 (finding that agent used a clear search methodology, only searching records where evidence might logically be found).

The court explained its divergence from the *Carey* dictum by explaining that because the scope of a computer search can never be less than the subject matter described in the warrant and affidavit, the limitations suggested in *Carey* cannot effectively restrict a computer search.[57] The objects of the government search can be hidden using misleading directory or file names[58] or disguised by false file extensions.[59] Keyword searches cannot confine a computer search because keyword searches are based on file names, which may be unreliable or inaccurate.[60] Even the file directory structure can be manipulated so as to obfuscate investigators, and the directory itself may simply be too confusing to provide a means of restricting the scope of a search.[61]

The court explained how its decision in *Burgess* was not inconsistent with *Walser* by explaining that even the most well-intentioned search protocol may eventually degenerate into general file-by-file rummaging.[62] The court stated, "[I]t is folly for a search warrant to attempt to structure the mechanics of the search,"[63] but asserted that this will not always be the case, admonishing that privacy rights require "an officer executing a search warrant to first look in the most obvious places and as it becomes necessary to progressively move from the obvious to the obscure."[64] The flaw in this statement became immediately apparent to the court: if an officer is to conduct a thorough search, and all of the limits identified in *Carey* may conceal legitimate search objects, then no search will be thorough unless it degenerates into a file-by-file general rummaging.[65] Thus, the court concluded, "in general a structured approach may provide only the illusion of protecting privacy interests."[66]

Despite concluding that "[t]he preview technique may be problematic in other contexts," the Tenth Circuit upheld the search.[67] First, the court praised Agent Hughes's decision to terminate his search as soon as he found evidence of criminal wrongdoing not specified by the warrant, and to secure a warrant with greater scope.[68] Part of *Carey*'s holding

[57] *Burgess*, 576 F.3d at 1092–93.

[58] *Id.* at 1093–94 & n.18 ("While file or directory names may sometimes alert one to the contents (*e.g.*, 'Russian Lolitas,' 'meth stuff,' or 'reagents'), illegal activity may not be advertised even in the privacy of one's personal computer—it could well be coded or otherwise disguised.").

[59] *See id.*

[60] *See id.* at 1093.

[61] *Id.* ("The directory structure might give hints as to an effective search strategy, but could just as well be misleading and most often could not effectively, or even reasonably, be described or limited in a warrant.").

[62] *See id.* at 1094.

[63] *Id.*

[64] *Id.*

[65] *See id.* (explaining that investigators may be required to search all computer folders and even preview files to ensure complete searches).

[66] *Id.* at 1095.

[67] *Id.* at 1094.

[68] *Id.* at 1094–95.

mandated this restriction on computer searches.[69] However, the court recognized that the only distinction between *Carey*'s requirement (to await a new warrant upon finding evidence outside the scope of the existing warrant) and no requirement at all, is that the files "would be discovered later, rather than earlier."[70] Second, the court reasoned that Agent Schmidt's affidavit included images of drugs as part of the search parameters, allowing Agent Hughes to look at image files.[71] Because Hughes began the search by looking at digital image files, the search conformed to the court's requirement that agents "first look in the most obvious places."[72] Third, because Hughes was allowed to search for photographs, he would inevitably have found the child pornography.[73] Finally, and tellingly, the court pointed out that Burgess[74] was unable to proffer a suitable alternative rule.[75]

II. THE COMPUTER–CONTAINER ANALOGY EXPANDS COMPUTER SEARCHES

The *Burgess* court discussed, in part, whether a computer may be directly analogized to a container.[76] Part II of this Comment examines the implications of a strict computer–container analogy, and argues that such treatment would significantly expand the ability of law enforcement to search a computer.[77]

A. The Automobile Exception

The Tenth Circuit discussed the automobile exception at considerable length in *Burgess*. Generally, people enjoy less privacy expectations in their cars than they do in their homes.[78] As the Supreme Court stated, "The Fourth Amendment does not treat a motorist's car as his castle."[79]

[69] *See* United States v. Carey, 172 F.3d 1268, 1276 (10th Cir. 1999).

[70] *Burgess*, 576 F.3d at 1095. Essentially, Hughes could have kept searching for photos of drugs and inadvertently discovered each and every instance of child pornography. *Id.*

[71] *Id.* at 1083–84, 1095.

[72] *Id.* at 1094. Although the court does not address it, some concern may be warranted over an agent trained in ferreting out child pornography immediately searching for evidence of drug distribution by looking at digital image files.

[73] *Id.* at 1095.

[74] This Comment argues that the Tenth Circuit could not come up with any good alternative either. *See infra* Part IV.

[75] *Burgess*, 576 F.3d at 1095.

[76] *Id.* at 1087–90.

[77] If the implications of a strict analogy of computers and containers are disturbing, the treatment of computer as a "virtual home" is untenable. In *California v. Carney*, the Supreme Court upheld a search of a vehicle under the automobile exception that served as the defendant's actual home. 471 U.S. 386, 392–94 (1985). Clearly in *Carney*, the amount of personal information stored within the defendant's motor home equated with that of an actual home. However, the Court applied not the enhanced protections associated with a home, but reduced protections associated with an automobile. If Carney's motor *home* did not deserve the heightened Fourth Amendment protection that the Court typically extends to homes, the idea that the Tenth Circuit was unwilling to extend heightened protection to Burgess's laptop computer should be utterly unremarkable.

[78] Carroll v. United States, 267 U.S. 132, 153 (1925).

[79] Illinois v. Lidster, 540 U.S. 419, 424 (2004).

The automobile exception permits an officer to search a vehicle without a warrant when that officer has probable cause to believe evidence or contraband may be found in the vehicle.[80]

Under *United States v. Ross*,[81] an officer with probable cause to search a vehicle could only extend the warrantless search to a container within the vehicle if the officer had probable cause to believe that the container "may conceal the object of the search."[82] The Supreme Court weakened that requirement in *California v. Acevedo*,[83] however, by allowing a warrantless search of a vehicle under the automobile exception to extend to containers within that vehicle regardless of whether probable cause exists for each individual container.[84] In *Wyoming v. Houghton*,[85] the Court clarified that an officer who has probable cause to search a vehicle may conduct a warrantless search of any container within the vehicle capable of concealing the sought items.[86] This rule extends to all containers found in a vehicle, regardless of the ownership of the container.[87]

As *Burgess* contemplates, a strict computer–container analogy would allow a warrantless search of any computer found in an automobile so long as the police have probable cause to search the vehicle itself. Under *Houghton*, the law would not distinguish between a computer owned by a passenger and one owned by the vehicle's owner. Thus, any digital storage device—regardless of its ownership—is subject to immediate, warrantless search by an officer who finds the device while executing a valid vehicle search, provided that the device is capable of concealing the items sought by the officer.

B. Search Incident to Arrest

In addition to expanding searches pursuant to the automobile exception, a strict computer–container analogy would likely to increase the number of computer searches incident to arrest. The U.S. Supreme Court explained the search incident to arrest doctrine in *Chimel v. California*,[88] where it established that an officer without a warrant may search the area within the arrestee's immediate control in order to protect officer safety and to prevent the destruction of evidence.[89] Under *New York v. Belton*,[90]

[80] *See Carney*, 471 U.S. at 388.
[81] 456 U.S. 798 (1982).
[82] *See id.* at 825.
[83] 500 U.S. 565 (1991).
[84] *See id.* at 574.
[85] 526 U.S. 295 (1999).
[86] *See id.* at 307.
[87] *Id.*
[88] 395 U.S. 752, 762–63 (1969).
[89] *Id.* at 763.
[90] 453 U.S. 454 (1981).

a *Chimel* search extends to an automobile if the arrestee is driving.[91] Therefore, under the rule in *Chimel*—and assuming a strict container–computer analogy regime—an officer's search of a laptop or digital storage device in the possession of a lawfully arrested person could be undertaken without a warrant.

The Supreme Court established a new rule for searches incident to arrest in *Arizona v. Gant*.[92] Under the *Gant* rule, a warrantless search incident to arrest of an automobile occupant is permissible when either the search is for evidence of the arresting offense or when the officer cannot secure the arrestees.[93] Justice Stevens, writing for the majority, left open the possibility that either search might be justified in contexts outside of a roadside vehicle stop.[94]

Because *Ross* allows an officer to search any container capable of containing the object of the search provided the container is found during a valid vehicle search,[95] the combination of *Ross* and *Gant* broaden the ability of police to search containers following an arrest. Taken together, the two cases allow an officer, after a lawful arrest for an evidence-based crime, to conduct a warrantless search for evidence of that crime throughout the arrestee's vehicle and in any container in that vehicle, so long those containers are capable of hiding the sought evidence. If Justice Steven's suggestion—that *Gant* may be the rule for *any* search incident to arrest—is correct, a container within the control of an arrestee is automatically subject to warrantless search so long as it could contain evidence of the arresting offense.

Extending the *Gant–Ross* rule to the digital evidence context, a computer must be capable of containing pertinent evidence of the crime before an officer is allowed to search it without a warrant. However, in this multimedia age, it is difficult to imagine a situation where a computer is incapable of containing evidence—such as photographs—of a crime. While it may be far-fetched to assert that a defendant or his passenger had taken digital photographs of a minor infraction such as a traffic violation, certainly such photographs are *capable* of existing on a computer.

III. PRIVACY EXPECTATIONS ON YOUR COMPUTER

While search doctrines that embrace the computer–container analogy will likely lead to a greater number of computer searches, police may access personal computer information in some instances without

[91] *Id.* at 460. The occasions which would trigger an automobile's search incident to arrest and the extent of that search has been limited by the Supreme Court in *Arizona v. Gant*, but the principle remains the same. 129 S. Ct. 1710, 1719 (2009).

[92] *Gant*, 129 S. Ct. at 1719.

[93] *Id.* at 1718–19.

[94] *Id.* at 1721.

[95] United States v. Ross, 456 U.S. 798, 825 (1982).

ever implicating the Fourth Amendment. In *Katz v. United States*,[96] Justice Harlan's concurrence defined a search as a violation of a legitimate expectation of privacy.[97] The question then, is when does a person have a legitimate expectation of privacy on their computer? Courts have generally held that a personal computer, in most circumstances, is not accessible by the public at large, and therefore subject to a reasonable expectation of privacy.[98] However, in some situations that expectation is stronger, and in some cases no legitimate expectation exists whatsoever.

A. File Sharing

It is axiomatic that public places are not subject to the same expectations of privacy as private places.[99] When a person uses file sharing software, they grant public access to the private content on their computer. In essence, a person using a program such as Napster or LimeWire to share files with the public may also be destroying a legitimate expectation of privacy in their computer. That was exactly the situation presented to the Eighth Circuit in *United States v. Stults*.[100] In *Stults*, the court held that the government's inspection of the defendant's downloads folder did not implicate the Fourth Amendment because the defendant's decision to use and install a file sharing program rendered that folder open to the public.[101] Conceivably, after *Stults*, a court would uphold a federal agent's suspicionless and warrantless search of any computer folder that is accessible by a file sharing program.

B. Deleted Files

The Supreme Court has also held that a warrantless search of items that a person has abandoned does not implicate the Fourth Amendment.[102] In *California v. Greenwood*, the Court held that a warrantless police search of sealed, opaque garbage bags left on the street did not rise to the level of a "search," in the meaning of *Katz*, because a person abandons any reasonable expectation of privacy by making items or information available to the general public.[103] Deleted computer files are not set out on the curb or otherwise available for public inspection. Nor are deleted computer files handed over to a third party for destruction. How-

[96] 389 U.S. 347 (1967).

[97] *Id.* at 360–61 (Harlan, J. concurring).

[98] *See, e.g.*, United States v. Young, 573 F.3d 711, 721 (9th Cir. 2009); United States v. Crist, 627 F. Supp. 2d 575, 585 (M.D. Pa. 2008); United States v. Barth, 26 F. Supp. 2d 929, 936 (W.D. Tex. 1998).

[99] *See, e.g.*, California v. Greenwood, 486 U.S. 35, 41–42 (1988) (holding search of garbage left on public streets warranted no legitimate expectation of privacy and did not implicate Fourth Amendment).

[100] 575 F.3d 834, 843 (8th Cir. 2009).

[101] *Id.* Interestingly, the defendant claimed he did not know that the program opened his computer to the public, yet the court still found that the defendant "opened his download folder to the world." *Id.*

[102] *Greenwood*, 486 U.S. at 41–42.

[103] *Id.* at 40–42.

ever, computers do have virtual trashcans, and the deleted items that occupy them are arguably abandoned. So, if the government conducts a search of a Windows Recycle Bin or a restoration and search of deleted files, is the Fourth Amendment implicated? According to the First Circuit, it is. In *United States v. Upham*,[104] the court found enough of a distinction between deleted computer files and trash bags left on the street to state that a computer user continued to have an expectation of privacy in deleted computer files.[105] Unlike garbage left on the street, where, conceivably, anyone may rifle through it, deleted computer files are not exposed to the public at-large.[106]

C. Password Protection and Encryption

Files protected by passwords or encryption are entitled to a greater level of privacy than those without such safeguards.[107] In *Trulock v. Freeh*, the Fourth Circuit held that protecting a computer with a password is an expression of intent to remain private, akin to placing a lock on a footlocker.[108] The Tenth Circuit has adopted this analogy.[109]

However, one commentator has suggested that there is no basis for granting heightened privacy rights to electronic information protected by encryption.[110] Professor Kerr analogizes encryption to the shredding of files or to speaking in foreign languages, both being scenarios in which no heightened level of privacy was granted.[111] Simply because individuals express their desire to hide their computer files behind encryption or their physical files by shredding does not mean that such a privacy expectation is legitimate enough for the government to be bound to acknowledge it.

IV. ELUSIVE LIMITS FOR COMPUTER SEARCHES

When the Fourth Amendment is implicated, a search must be conducted under the auspices of a warrant or pursuant to one of the excep-

[104] 168 F.3d 532 (1st Cir. 1999), *cert. denied sub nom.* Upham v. United States, 527 U.S. 1011 (1999).

[105] *Id.* at 537 n.3.

[106] *Id.* ("We reject the government's suggestion that, by deleting the images, Upham 'abandoned' them and surrendered his right of privacy. Analogy is a hallowed tool of legal reasoning; but to compare deletion to putting one's trash on the street where it can be searched by every passer-by is to reason by false analogy." (citations omitted)).

[107] *See, e.g.*, Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir. 2001).

[108] *Id.*

[109] United States v. Andrus, 483 F.3d 711, 718 (10th Cir. 2007) ("Because intimate information is commonly stored on computers, it seems natural that computers should fall into the same category as suitcases, footlockers, or other personal items that 'command[] a high degree of privacy'" (alteration in original) (quoting United States v. Salinas-Cano, 959 F.2d 861, 864 (10th Cir. 1992))).

[110] Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?,"* 33 CONN. L. REV. 503, 505 (2001).

[111] *Id.* at 513–18 (citing United States v. Longoria 177 F.3d 1179, 1183 (10th Cir. 1999) (foreign languages); United States v. Scott, 975 F.2d 927, 928 (1st Cir. 1992) (shredding)).

tions to the warrant requirement. When the government conducts a search of computer files in the context of a validly issued search warrant, the scope of the search must be limited to those things particularly described by the warrant. However, as *Burgess* recognizes, narrowing the scope of a lawful search of a computer becomes difficult, if not impossible. This section examines the problem of scope and generality in computer searches.

A. The Plain View Doctrine

Under the plain-view doctrine, if an officer conducting a lawful search uncovers an item that is obviously contraband or evidence, the officer may seize that item.[112] However, as the *Burgess* court emphasized, the owner of a computer may have masked the location or nature of contraband through creative use of file names, extensions, and directory structure. Accordingly, a search of a computer ultimately must be conducted in a manner which renders the entire contents of a hard drive in "plain view."[113] As Professor Kerr has stated, the plain view exception "does not impose a real limit on searches for electronic evidence . . . . Because electronic evidence can be located anywhere on a hard drive, it is difficult, if not impossible, to say that a physical search was objectively unjustifiable."[114]

B. File names and Extensions

One limitation on searches for digital evidence could be file names. Often file or folder names speak to their contents. For example, the Sixth Circuit found that an informant's tip that a defendant had a folder on his computer titled "child kiddie" provided, in part, the basis for probable cause for a warrant to search that computer.[115] However, *Burgess* rejects the converse proposition: that a search can be restricted to files with suspicious names.[116] The Tenth Circuit argues that file names can easily be changed to disguise their contents.[117]

Another limitation could be file extensions. File extensions are "tags" appended to file names that indicate to the computer and the user what type the file is. Presumably, a search could be restricted to files that exhibit specific file extensions. For instance, a search for child pornography could be limited to image files with extension types such as .gif, .jpeg, and so on.

[112] Coolidge v. New Hampshire, 403 U.S. 443, 464–66 (1971).

[113] *See* United States v. Burgess, 576 F.3d 1078, 1095 (10th Cir. 2009).

[114] Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 305 (2005).

[115] United States v. McNally, 327 F. App'x 554, 557–58 (6th Cir. 2009).

[116] *Burgess*, 576 F.3d at 1092–94.

[117] *Id.* at 1093.

The *Burgess* court rejected this limitation as well.[118] Like file names, it reasoned, file extensions can be manipulated to conceal a file's true nature, and a wide variety of file extensions can hold the type of information sought by authorities.[119] This argument was also advanced by the United States District Court for the Eastern District of Virginia in *United States v. Gray*.[120] There, the court asserted, as did the *Burgess* court, that file names and extensions cannot limit the scope of a proper search of a computer.[121]

C. Restrictions of Search Methodology

Professor Kerr has suggested that one means of limiting the scope of computer searches is to require police to have their search methodology pre-approved by a magistrate.[122] However, *Burgess* explains that any search protocol for a computer will ultimately degrade into a general search.[123] At first blush, keyword searches may seem like an acceptable method of restraining a computer search. But, as the *Burgess* court expressed, such searches are often based on file names,[124] and if file names may be modified to conceal legitimate objectives of a search, keyword searches are just as unreliable.[125] Similarly, requiring officers to search a computer based on the manner in which the files are organized does nothing to eliminate the possibility that pertinent evidence could be concealed in an unintuitive location on the drive; as a result, authorities can present a colorable argument of the necessity to search everywhere on the drive.[126] Indeed, Professor Kerr asserts, "The physical-world rules do not prevent a general rummaging through electronic evidence."[127]

But even the *Burgess* court fell into the trap of trusting prescribed methodologies to limit computer searches. The court stated:

> A warrant may permit only the search of particularly described places and only particularly described things may be seized. As the

[118] *Id.*

[119] *Id.*

[120] 78 F. Supp. 2d 524, 529 (E.D. Va. 1999).

[121] *Id.*

[122] *See* Kerr, *supra* note 114, at 316 (citing *In re* Search of 3817 W. West End, 321 F. Supp. 2d 953 (N.D. Ill. 2004)).

[123] *See Burgess*, 576 F.3d at 1094.

[124] While forensic search engines such as dtSearch look for keywords inside of text-based documents giving some clue as to their genuine contents, this is not the case in digital photographs where no or limited text is associated with the file's contents. *See* Beryl A. Howell, *Digital Forensics: Sleuthing on Hard Drives and Networks*, VT. B.J., Fall 2005, at 39, 42–43.

[125] *See Burgess*, 576 F.3d at 1093–94. *See generally* Susan W. Brenner & Barbara A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 MICH. TELECOMM. & TECH. L. REV. 39, 60–61 (2002) (examining the limitations of automated searches on computers).

[126] The *Burgess* court mocks this notion, stating: "One would not ordinarily expect a warrant to search filing cabinets for evidence of drug activity to prospectively restrict the search to 'file cabinets in the basement' or to file folders labeled 'Meth Lab' or 'Customers.' And there is no reason to so limit computer searches." *Burgess*, 576 F.3d at 1094.

[127] Kerr, *supra* note 114, at 305.

> description of such places and things becomes more general, the method by which the search is executed become[s] more important—the search method must be tailored to meet allowed ends.[128]

However, the court's suggestion of a limiting principle is simply to look in obvious places first and less obvious places second, which is truly no limit at all.[129] Instead, such methodology is a means of expediting—rather than limiting—searches. As the court conceded, "a structured approach may provide only the *illusion* of protecting privacy interests."[130]

D. Generality and Heterogeneity

The holdings of *Burgess* and *Gray* create a scenario where the permissible search of a computer for any one file automatically permits law enforcement to search all files on the computer, effectively turning a particularized warrant—where one exists—into a general warrant whenever a computer file is specified.[131] This problem exists, in part, because computers contain many heterogeneous files, most of which will not be responsive to any given search.

This problem of heterogeneous records is not new to computers. The Supreme Court has considered it in the context of searches of file cabinets. In *Andresen v. Maryland*, the Supreme Court stated:

> We recognize that there are grave dangers inherent in executing a warrant authorizing a search and seizure of a person's papers that are not necessarily present in executing a warrant to search for physical objects whose relevance is more easily ascertainable. In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized. Similar dangers, of course, are present in executing a warrant for the "seizure" of telephone conversations. In both kinds of searches, responsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy.[132]

Like papers and phone records, searches of computer records inevitably cause non-responsive documents to be swept up with responsive

[128] *Burgess*, 576 F.3d at 1094.

[129] *Id.*

[130] *Id.* at 1095 (emphasis added).

[131] This generality problem is exacerbated by the *Upham* decision. *See supra* Part III.B. The *Upham* court held that a warrant authorizing a search of defendant's computer implicitly authorized federal agents to restore and search deleted files on the computer. United States v. Upham, 168 F.3d 532, 537 n.3 (1st Cir. 1999), *cert. denied sub nom.* Upham v. United States, 527 U.S. 1011 (1999). Any method of "extract[ing]" the information sought, said the court, was permissible. *Id.* at 536. Putting *Burgess* and *Upham* together, a search of any computer for a single file authorizes a search of every file including those deleted files, which may be—by any means—recovered.

[132] 427 U.S. 463, 482 n.11 (1976).

files. The Court permits files to be examined so investigators may determine whether those files are authorized for seizure—indeed, this is what occurred in *Burgess*.[133] However, the Court's admonition that this search be "conducted in a manner that minimizes unwarranted intrusions upon privacy"[134] must not be ignored. Searching a computer by peering into the contents of every folder and every file is perhaps the method that *least* minimizes "unwarranted intrusions upon privacy." In fact, the Court's language in *Andresen* may preclude investigators from conducting the type of search performed in *Burgess* and *Gray* so long as there are less intrusive methods available. Furthermore, purporting to limit a general search by requiring it to start at the most obvious location but ultimately allowing it to wander through the entire contents of a hard drive cannot be seen as meeting *Andresen*'s minimization requirement because the privacy violation, in the end, is identical to that of a general search of the hard drive. The sanctioning of this approach exemplifies the type of illusory protection employed by the *Burgess* court.

Aside from asking the investigators to begin their search in the most obvious location, the Tenth Circuit provided a second—and equally illusory—protection. When Agent Hughes found the first image of child sexual exploitation on David Burgess's hard drive he stopped searching and obtained an expanded warrant that included permission to search for additional child pornography.[135] Hughes' original search was constrained by the scope of the first warrant; which was designed to adhere to the Tenth Circuit's decision in *Carey*. In *Carey*, the court held that in order to utilize the plain view doctrine in searches of electronic records, an officer must obtain an additional warrant upon discovering contraband not particularly described in the original warrant.[136] The *Carey* court found that an officer conducting a warranted computer search for drug evidence violated the Fourth Amendment when he exceeded the scope of the warrant by extending his search to look for additional child pornography after identifying an initial image.[137] In contrast, the *Burgess* court commended Agent Hughes for securing additional authority to search for child pornography, but admitted that Hughes could have gone on searching as long as he was still searching for photos of drugs or anything else within the scope of the original warrant.[138] In other words, Hughes could have searched so long as his subjective intention was to find pictures of drugs and not child sexual exploitation.[139]

[133] *Id.*

[134] *Id.*

[135] *Burgess*, 576 F.3d at 1084.

[136] United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999).

[137] *Id.* at 1271, 1276.

[138] *Burgess*, 576 F.3d at 1095.

[139] *See id.* Looking at the subjective intent of an officer conducting a search is an oddity in Fourth Amendment jurisprudence. *See generally* Whren v. United States, 517 U.S. 806 (1996) (holding that an officer's subjective reasons for a vehicle stop are irrelevant).

While the *Burgess* court's response to the *Carey* rule is tepid,[140] from a privacy standpoint there is even less reason to celebrate such a rule. To begin with, if officers can search until they find contraband outside the scope of their warrant, but can use that contraband to retroactively secure an expanded warrant and continue searching for similar contraband, it is unclear what additional limit that places on an electronic search. Second, *Burgess* stands for the proposition that an officer searching a computer for tax records who finds photos of drugs has merely to state that they are still searching for tax records as they systematically (and inadvertently, of course) stumble across every photo of drugs on the hard drive.[141] Last, an officer who complies with the *Carey* rule and stops searching after finding the first instance of contraband not covered by the warrant will inevitably discover all contraband on the computer after securing an additional warrant. Thus, even if officers fail to stop and secure a warrant, modern rules of criminal procedure would prevent any evidence so obtained from being excluded from evidence in a later trial.[142] Accordingly, the requirement to stop an ongoing search upon discovering unexpected contraband to secure an expanded warrant is a wholly illusory protection, ultimately granting no greater limitation on the scope of a computer search than having no requirements at all.

V. The Ninth Circuit Provides a Solution: Third Party Review

On one hand, courts reject general warrants and general searches.[143] However, cases like *Gray* and *Burgess* stand for the proposition that—by necessity—a search of a computer for any one thing can easily degenerate into a general search of the computer's contents. *Andresen* states that this is permissible so long as no alternative exists that would generate fewer privacy invasions. But is there truly no alternative to allowing officers free reign whenever they have cause to search a computer?

In *United States v. Comprehensive Drug Testing, Inc.*,[144] the Ninth Circuit Court of Appeals created such an alternative. *Comprehensive Drug Testing* outlined a new rule requiring third-party review and redaction of computer files, which restricts, while not crippling, law enforcement's access to personal computer files.[145]

[140] *See Burgess*, 576 F.3d at 1092 ("[I]t is tempting . . . to over read *Carey*. But the *Carey* holding was limited.").

[141] *See id.* This subjective standard creates a perverse incentive for officers to lie about what their intentions are while searching a computer.

[142] According to the so-called inevitable discovery exception to the exclusionary rule, this type of evidence could be introduced to trial. *See generally* Nix v. Williams, 467 U.S. 431 (1984) (holding that exclusion of evidence initially obtained illegally, but which would have been inevitably discovered, is contrary to purpose of exclusionary rule).

[143] *See, e.g.*, Maryland v. Garrison, 480 U.S. 79, 84 (1987).

[144] 579 F.3d 989 (9th Cir. 2009) (en banc).

[145] *Id.* at 1006.

A. Background

Guided by suspicions that Bay Area Lab Cooperative ("BALCO") had supplied controlled steroids to professional baseball players, the federal government launched an investigation into the lab in 2002.[146] That same year, Major League Baseball ("MLB") entered into an agreement with the Major League Baseball Player's Association to conduct random, suspicionless drug testing of players.[147] According to the agreement, urine samples were collected and tested for banned substances, and the results would remain anonymous and confidential.[148] MLB employed Comprehensive Drug Testing, Inc. ("CDT") to independently administer the testing program.[149]

Federal investigators learned of ten players that had tested positive in the CDT program.[150] The government obtained a subpoena for all drug testing records and specimens pertaining to MLB in CDT's possession.[151] In response, CDT and the players moved to quash the subpoena.[152] Subsequently, federal authorities obtained a warrant authorizing the search of CDT's facilities for evidence relating to the ten players suspected by federal investigators of steroid use.[153] However, the government, conducting the search, promptly seized and searched all of the drug testing records, including the test results of hundreds of MLB players and of "a great many other people."[154]

In response, CDT and the players moved for return of the drug testing records.[155] The players prevailed at the District Court level.[156] A three-judge panel in the Ninth Circuit Court of Appeals affirmed in part

[146] *Id.* at 993.

[147] *Id.*

[148] *Id.*

[149] *Id.* CDT, in turn, hired Quest Diagnostics, Inc. ("Quest") to conduct blind testing wherein CDT retained the names of the players and the sample results, while Quest did the actual testing, retaining the samples. *Id.*

[150] *Id.*

[151] *Id.*

[152] *Id.*

[153] *Id.*

[154] *Id.*

[155] *Id.* The players invoked Federal Rule of Criminal Procedure 41(g) which provides:

> A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return. The motion must be filed in the district where the property was seized. The court must receive evidence on any factual issue necessary to decide the motion. If it grants the motion, the court must return the property to the movant, but may impose reasonable conditions to protect access to the property and its use in later proceedings.

FED. R. CRIM. P. 41(g).

[156] *Comprehensive Drug Testing*, 579 F.3d at 993–94. Judge Cooper in the Central District of California granted the motion, stating that federal authorities had failed to comply with the terms of the original warrant, and ordered the return of the records (the "Cooper Order"). *Id.* CDT and the players also obtained a similar order from Judge Mahan in the District of Nevada relating to the records and samples seized under warrants issued by that court (the "Mahan Order"). *Id.* at 994. CDT and the players moved to quash the subpoenas, and Judge Ilston in the Northern District of California quashed the subpoenas (the "Illston Quashal"). *Id.*

and reversed in part.[157] The Ninth Circuit then voted to hear the case en banc.[158]

B. The Ninth Circuit Faces the Scope of a Computer Search Problem

Similar to the *Burgess* court, the Ninth Circuit was confronted with the problem of a search for a single document or group of documents on a computer degenerating into a general search of the computer's hard drive. The Ninth Circuit had dealt with heterogeneous searches before in *United States v. Tamura*.[159] In that case, the court permitted the government to seize a number of boxes of paper files in order to sort through and segregate the pertinent evidence.[160] *Tamura* can be analogized with *Carey*: in both cases, procedural requirements were imposed on a search of heterogeneous records and in both cases the government ultimately obtained total access to all documents.[161] However, the Ninth Circuit recognized that *Tamura* was never intended to be applied to digital evidence cases.[162] The court emphasized that digital evidence cases, unlike *Tamura*, do not merely "involve[] a few dozen boxes," but rather "millions of pages of information."[163] Further, *Tamura* was anticipated to be the rare exception, yet with the increasing prevalence and importance of digital evidence, heterogeneous searches can hardly be considered rare exceptions.[164] With the understanding that the *Tamura* exception would fast swallow the rule, the court updated its heterogeneous searches jurisprudence, recognizing "the daunting realities of electronic searches."[165]

In considering this change, the court attempted to balance two interests. On one hand the court recognized that because computer records are heterogeneous, government searches of computers will inevitably sweep up large amounts of nonresponsive personal information.[166] As the court stated, "over-seizing is an inherent part of the electronic search process."[167] Furthermore, as the *Burgess* court identified, legitimate objectives of searches may be concealed based on file names, directory structure, or file extension, requiring a diligent officer to expand her search to the entirety of the digital storage device.[168]

[157] *Id.* The panel upheld the Cooper Order on the grounds the appeal was untimely. *Id.*

[158] *Id.*

[159] 694 F.2d 591 (9th Cir. 1982).

[160] *Id.* at 595.

[161] *See* Donald Resseguie, Note, *Computer Searches and Seizure*, 48 CLEV. ST. L. REV. 185, 209–10 (2000) (critiquing *Tamura*'s failure to restrict the scope of a computer search).

[162] *See Comprehensive Drug Testing*, 579 F.3d at 996 ("*Tamura*, decided in 1982, just preceded the dawn of the information age . . . .").

[163] *Id.* at 1004.

[164] *Id.* at 1006.

[165] *Id.*

[166] *Id.* at 1004, 1006.

[167] *Id.* at 1006.

[168] *See id.* at 1004.

On the other hand, computers contain vast amounts of personal information about their owners, and—in many cases, such as email servers—of many other people.[169] Modern Americans, said the Ninth Circuit, have no choice but to have personal information on the computers of others.[170] Subjecting these servers to the type of limitless computer search endorsed by *Burgess* could result in the violation of the privacy of millions of other potentially innocent people.[171]

Balancing these two interests, the court created five requirements to restrict the scope of computer searches[172]: (1) the government should waive the plain view doctrine in digital evidence cases; (2) seized files must be segregated and redacted by specialized or independent personnel in such a way that the government does not have free access to the materials; (3) warrants and subpoenas must include the government's history of seeking that information as well as the actual risk that the information will be destroyed; (4) the government must tailor its search in order to uncover only that information for which it has probable cause; and (5) the government may not keep non-responsive data, and must keep the magistrate informed as to what it does and does not keep.[173]

Comprehensive Drug Testing's second requirement requires the government to hire a third party or specialized computer personnel to review and redact nonresponsive information from the search.[174] In either case, the personnel may not divulge any nonresponsive information to law enforcement.[175] This requirement provides real—not illusory—privacy protections. The third party will have the ability to perform the general search that the *Burgess* court finds inescapable, but the information exhumed by such a search can only be used by law enforcement if it meets the particulars of a warrant. Arguably, this standard is onerous, depriving law enforcement of important evidence that may not be otherwise obtainable. Indeed, two circuits have recently made that argument.

*C.*Comprehensive Drug Testing*'s Impact on Subsequent Cases*

1. The Seventh Circuit: *United States v. Mann*[176]

After *Comprehensive Drug Testing*, the Seventh Circuit Court of Appeals grappled with digital evidence in *United States v. Mann*. In *Mann*, police discovered child pornography while searching Mann's computer pursuant to a warrant for digital evidence of voyeurism, and proceeded to search the entire computer without a grant of additional

[169] *Id.* at 1004–05.
[170] *Id.* at 1005.
[171] *See id.*
[172] *Id.* at 1006.
[173] *Id.*
[174] *Id.*
[175] *Id.*
[176] 592 F.3d 779 (7th Cir. 2010).

authority.[177] The court distinguished *Carey* by noting that the searching officer in *Mann*, despite finding child pornography, never stopped looking for evidence of voyeurism.[178] In effect, the Seventh Circuit thus applies *Carey* only in cases where the officer subjectively intended to exceed the scope of the warrant. This rule fails to provide substantive computer privacy protections for three reasons. First, the rule opens up computer searches to *ex-post facto* justifications by officers. Second, the Supreme Court has long held that subjective motivations by officers are irrelevant to Fourth Amendment analysis.[179] Finally, even if the officer is required to comply with *Carey* by securing additional search authorization, this rule, as discussed *supra*, does little to limit the scope of a computer search.[180]

The *Mann* court also rejected the *Comprehensive Drug Testing* rule, reaffirming the plain view doctrine's role in digital evidence cases.[181] However, the court signaled its displeasure at the state of digital evidence jurisprudence, disagreeing with the substance of the *Comprehensive Drug Testing* rule but not its purpose.[182] To the *Mann* court, the *Comprehensive Drug Testing* rule was "efficient but overbroad" and instead suggested that less severe rules would develop incrementally "through the normal course of fact-based case adjudication."[183] However, the *Burgess* court, by failing to build on the electronic search limitations established in *Carey* and *Walser*, demonstrates the problems an incremental approach presents. As Professor Kerr has argued, physical-world rules of criminal procedure cannot simply be built up—incrementally or otherwise—to create meaningful protections of digital privacy.[184]

2. The Fourth Circuit: *United States v. Williams*[185]

In *Williams*, the Fourth Circuit took a different approach. Digital searches, the court held, are not distinguishable from other searches.[186] Accordingly, the court rejected even the illusory protections of *Carey*.[187] Under the *Williams* rule, a search of digital evidence pursuant to a valid warrant is no different than any other search.[188] To the Fourth Circuit, digital evidence presents no different a situation than the mixed records

[177] *Id.* at 781.

[178] *Id.* at 784.

[179] *See* Whren v. United States, 517 U.S. 806, 816–17 (1996).

[180] *See supra* Part I.B.2.

[181] *Mann*, 592 F.3d at 785–86.

[182] *See id.*

[183] *Id.* (internal quotation marks omitted) (quoting United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 1013 (9th Cir. 2009) (en banc) (Callahan, J., concurring in part and dissenting in part)).

[184] *See* Kerr, *supra* note 114, at 280.

[185] 592 F.3d 511 (4th Cir. 2010).

[186] *Id.* at 523–24.

[187] *Id.* at 523.

[188] *See id.* at 524.

problems that cases like *Tamura* were tailored to address.[189] While this understanding avoids propping up illusory protections, it does so by providing little—if any—in the way of computer privacy protections.

The approaches of the Fourth and Seventh Circuits fail to resolve the problem that frustrated the *Burgess* court. On one hand, the Fourth Circuit appears satisfied that no additional safeguards are necessary to protect computer privacy, a position that at least does not create the illusion of computer privacy where none exists. On the other hand, the Tenth and Seventh Circuits both agree that digital evidence requires additional privacy protections, yet those courts either cannot find a way to implement meaningful protections or decline to do so. If courts claim to believe that privacy protections are needed for digital evidence cases, those courts should reject illusory and incremental approaches and adopt substantive protections; to date, only the Ninth Circuit has done so.

Like the Tenth Circuit's rules in *Carey*, *Burgess*, and *Walser*, the Ninth Circuit's holding in *Tamura* imposed only illusory privacy protections, ultimately permitting a general search of a heterogeneous record.[190] The Ninth Circuit recognized in *Comprehensive* that an outdated approach that assumes heterogeneous records are the exception, and not the norm, cannot be justified in a modern context.[191] The Supreme Court's dictum in *Andresen*, which directs officers to "minimize[] unwarranted intrusions upon privacy" when searching files may mean that the rules stated by the Ninth Circuit—or some lesser version thereof—are constitutionally mandated.[192] The Ninth Circuit's *Comprehensive Drug Testing* decision requires the government to waive the plain view doctrine.[193] While the Seventh Circuit criticizes this approach as "efficient, but overbroad,"[194] the Ninth Circuit's rule at least provides meaningful protections to computer privacy. If the Tenth Circuit cannot justify any meaningful protections, then it should—as the Fourth Circuit has—openly admit this. On the other hand, if digital privacy is important to the Tenth Circuit, the court should look to the Ninth Circuit for an example of how to create meaningful protections.

CONCLUSION

As long as courts such as the Tenth Circuit decline to confront the unique Fourth Amendment implications of computers and electronic evidence, lower courts are likely to suffer the same pitfalls as the *Bur-*

[189] *See id.*

[190] *See* United States v. Tamura, 694 F.2d 591, 595–96 (9th Cir. 1982); *see also* Resseguie, *supra* note 161, at 209–10.

[191] United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 1004–05 (9th Cir. 2009) (en banc).

[192] Andresen v Maryland, 427 U.S. 463, 482 n.11 (1976).

[193] *Comprehensive Drug Testing*, 579 F.3d at 1006.

[194] United States v. Mann, 592 F.3d 779, 785–86 (7th Cir. 2010).

gess court. This result will have troubling consequences for our increasingly electronic society. Treating a computer as a container will ultimately result in more warrantless searches of computers. This consideration is exacerbated by the difficulty of providing meaningful limits to legitimate searches of digital evidence as discussed in *Burgess*. Indeed, if police are allowed to access computers in the same manner as any other container, and their access to electronic files cannot be meaningfully limited, an individual's most personal digital files will be increasingly exposed to law enforcement. Accordingly, an individual's personal computer files are now subject to a low threshold for discovery by lawful search or accident. Rather than admit that an individual can expect their private files to often get swept up with legitimate digital search objectives, however, the Tenth Circuit indefensibly relies on the illusion of privacy protection in computers.

The Ninth Circuit advanced a substantive protection of computer privacy in *Comprehensive Drug Testing*. Third party review and redaction allows police to access information for which they have probable cause, without giving law enforcement carte blanche to examine nonresponsive or irrelevant private computer files. The expanding role of computers in modern life, the *Andresen* dictum requiring the minimization of privacy infringements, and the example of the Ninth Circuit should push other courts, including the Tenth Circuit, to update their decade-old heterogeneous search rules to address these realities—or, at the very least, assert their rejection of computer privacy in plain terms.

Darren Kafka[*]

[*] J.D. Candidate 2011, University of Denver Sturm College of Law. I would like to thank Professor Justin Marceau for his invaluable encouragement and advice. I would also like to thank David Frommell and the rest of the staff and editors of the *Denver University Law Review* for their tremendous efforts in improving this comment. I want to recognize the many years of support, love and inspiration from my father, mother, my brother Mark, and, most of all, from Lise: Thank you for believing in me.