DIGITIZING THE FOURTH AMENDMENT: LIMITING THE PRIVATE SEARCH EXCEPTION IN COMPUTER INVESTIGATIONS

* Benjamin Holley*

Our lives increasingly rely on computers: for work, for play, for learning, and for socializing. Accordingly, more and more personal information is stored on those computers. Yet these machines on which we depend are vulnerable: hardware and software can fail, virtual intruders can compromise our privacy, and thieves can walk away with our digital lifeline to the world. While all of these situations are frustrating, none seem to raise novel criminal procedure questions. What if, however, a third party turns over someone’s data to the police? For example, if a repair technician finds an image of child pornography on a computer, must the police, absent a warrant, limit themselves to viewing just that file, the folder it was in, or may they search the entire computer? What if the third party gained access to the files not by agreement with the computer owner but by “hacking”? And to what extent should the police be held responsible for the actions of these third parties? In our increasingly online world, these questions—raising issues of privacy, crime control, and constitutional law—will only become more common. Yet courts considering police re-creations of private computer searches have thus far developed widely varying approaches with dramatically different implications.

Each question above relates to the “private search exception” of the Fourth Amendment. It is well-established that government agents may, without a warrant, re-create a search that was originally conducted by a private individual, so long as they do not ex-

* Assistant State’s Attorney, McLean County, Illinois. J.D., 2009, University of Virginia School of Law; B.A., 2006, Truman State University. The views expressed in this Note are the author’s alone and do not necessarily reflect the views of the Office of the McLean County State's Attorney. Thanks to the staff of the Virginia Law Review for their hard work and helpful comments and to Renée Gordon Holley for her patience and proofreading acumen.
ceed the scope of that original search. Judicial opinions applying the private search exception to computer cases have, however, developed conflicting approaches as to both agency (that is, who qualifies as a government agent) and scope (that is, what precisely the government may view), and no clear standards predominate. Commentators have noted this inconsistency, and some have offered short analyses, but none have published an in-depth examination of the varying approaches to, and possible solutions for, this conflict. This Note attempts to fill that gap by examining various judicial efforts to apply the private search exception to modern technology, discussing the merits of each, and proposing solutions that maintain the spirit of the exception without sacrificing governmental interests or diminishing privacy rights. Specifically, it argues that because of the unique nature of computer technology, courts should broadly construe the agency prong and narrowly interpret the scope prong of the private search exception in computer search situations.

Part I provides necessary background information relating to both the private search exception and the structure of modern computers. Part II notes the difficulties courts have encountered in applying the first prong of the private search exception—agency—to computer cases. Part III follows by examining the difficulties inherent in the second prong of the exception—scope—and how the

---

1 See, e.g., Paul G. Reiter, Annotation, Admissibility, In Criminal Case, of Evidence Obtained by Search by Private Individual, 36 A.L.R.3d 553, 557–58 (1971); see also infra Section I.A.


3 Thomas K. Clancy, The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer, 75 Miss. L.J. 193, 236–44 (2005); Orin S. Kerr, Searches and Seizures in a Digital World, 119 Harv. L. Rev. 531, 547–48 (2005) (advocating an “exposure-based approach”); James M. Rosenbaum, In Defense of the Sugar Bowl, 9 Green Bag 2d 55, 55–56 (2005) (examining the scope problem in terms of the particularity requirement for warrants). Even those commentators who propose solutions to the conflict focus primarily on the Fourth Amendment requirement that warrants “particularly describ[e] the place to be searched, and the persons or things to be seized.” Id. at 55 (quoting U.S. Const. amend. IV). Though the debate regarding warrant specificity is relevant, this Note focuses on non-warrant private search exception situations, which turn on the scope of the private search versus the government agent search. These issues are slightly, but importantly, different.
subtle differences between courts’ varying approaches actually have dramatic implications. Part IV argues that courts should interpret the agency prong broadly and the scope prong narrowly. Finally, Part V anticipates possible objections to this conclusion and offers some replies.

I. BACKGROUND

A. Private Search Exception

Though ratified in 1791, the Bill of Rights has withstood the march of time remarkably well, even as courts have struggled to adapt the amendments’ protections to an ever-changing society unimaginable to the Founders. This struggle continues as courts attempt to harmonize the Fourth Amendment’s protection of “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures” with modern investigations and prosecutions of crime. As technology has evolved, the Supreme Court has added several nuances to the warrant requirement by creating new exceptions and expanding the scope of others. All the while, the Court has sought to balance citizens’ rights with the government’s need to enforce the laws. One warrant exception, applicable in both the “real” and virtual worlds, is the private search exception.

The private search exception contains two prongs: (1) the initial search must not be made by an agent of the government, and (2) the subsequent government search must not be “significantly more intrusive or extensive than the earlier private search.” If either

4 U.S. Const. amend. IV.

5 See, e.g., Carroll v. United States, 267 U.S. 132 (1925) (discussing the automobile exception).


prong is not satisfied, the government may not use the discovered evidence in trial.

The first prong—agency—arises out of the fact that the Fourth Amendment only constrains government action. Therefore, “it is wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official.” Accordingly, the government may use information obtained by private individuals, even if the individual violated the law to obtain it.

The Supreme Court has not clearly indicated the circumstances under which the government is considered responsible for private conduct, offering only the vague guideline that the result “necessarily turns on the degree of the Government’s participation in the private party’s activities, . . . a question that can only be resolved ‘in light of all the circumstances.’” Lower courts have adopted two approaches. The first applies a three-factor test, asking (1) “whether the government knew of and acquiesced in the intrusive conduct”; (2) “whether the private party’s purpose in conducting the search was to assist law enforcement”; and (3) “whether the government requested the action or offered the private actor a reward.” The alternative approach simply drops the third factor.

sofar as “the legality of the governmental search must be tested by the scope of the antecedent private search”).

See Reiter, supra note 1, at 561–62 (listing numerous state and federal cases agreeing with this proposition).

Jacobsen, 466 U.S. at 113 (quoting Walter, 447 U.S. at 662 (Blackmun, J., dissenting)) (internal quotation marks omitted). But see United States v. Allen, 106 F.3d 695, 698–99 (6th Cir. 1997) (suggesting in dicta that Jacobsen does not permit law enforcement to reenact a private search of a private home or residence).

For an argument against this rule in computer-based cases, see Monica R. Shah, Note, The Case for a Statutory Suppression Remedy to Regulate Illegal Private Party Searches in Cyberspace, 105 Colum. L. Rev. 250 (2005).


Crowley, 285 F.3d at 558 (internal citations omitted).

See, e.g., United States v. Miller, 688 F.2d 652, 657 (9th Cir. 1982).
The second prong—scope—rests on the theory that once a private individual searches another’s possessions, the owner’s expectation of privacy has been destroyed. Therefore, “the Fourth Amendment does not prohibit governmental use of the now non-private information.” However, “if the authorities use information with respect to which the expectation of privacy has not already been frustrated,” the traditional Fourth Amendment protections apply.

To avoid venturing into entirely uncharted territory, courts have sought analogies from “real world” law to apply to digital search cases. The most common involve a term found throughout Fourth Amendment precedent: “containers.” This term is well-defined for physical world law, but as will be seen, has no agreed-upon definition in the digital world. In traditional analysis, a container is simply “any object capable of holding another object,” and the Supreme Court has so far refused to treat different types of containers differently. Importantly, every opening of a container constitutes a separate search, so the government must produce a justi-
fication for each one. The complex nature of computer storage makes application of this analogy in the digital setting problematic. To determine the best approach, it is first necessary to understand the basics of computer storage.

B. Computer Architecture

Modern computers are able to store vast amounts of information, equal to approximately eighty million pages of text, with capacity doubling approximately every two years. For context, this is more information than is contained in one floor's worth of academic journals in the average university library.

To users, computer files appear to be stored within folders. Each folder may contain very few (or no) files or may contain thousands of files. Unlike a physical folder, virtual folders are functionally unlimited in size. Moreover, they are stored hierarchically, containing both files and folders within them. Thus, to extend the container analogy, computer folder systems are like matryoshka

---

24 Id. at 537. This is generally not an issue, as officers may open any container that could hold the evidence for which they are authorized to search. See also Rosenbaum, supra note 3, at 55.

25 See G. Robert McLain, Jr., Casenote, United States v. Hill: A New Rule, but No Clarity for the Rules Governing Computer Searches and Seizures, 14 Geo. Mason L. Rev. 1071, 1091 (2007) (“[T]he ‘technical’ aspects of computer storage are as relevant in formulating sound Fourth Amendment rules as the practical considerations that gave rise to the traditional rules governing container searches. Knowing how evidence is ‘contained’ on computers, and what kind of searches can discover evidence is essential to understanding whether the technical distinctions between computers and other containers should result in legal distinctions in Fourth Amendment search and seizure rules.”).

26 See Kerr, supra note 3, at 542 (calculating computer storage capacity in 2005 at forty million pages of text).


29 The only limit comes from the amount of storage space remaining on the medium on which the folders are themselves contained.
dolls—to open one closed container, one must often open another first.

While this is how the system appears to most users, data are not actually stored based on a hierarchy of folders. Indeed, forensic computer searches typically search and display the data in a different manner. Law enforcement officers conducting systematic searches of seized computers usually “image” the hard drive by creating bitstream copies. A bitstream image does not merely replicate each file and folder, but copies every bit of information in exactly the same order as it is on the original machine. This “physical level” differs from the “virtual level” generally seen by users. As one commentator explains:

A bitstream copy is different from the kind of copy users normally make when copying individual files from one computer to another. A normal copy duplicates only the identified file, but the bitstream copy duplicates every bit and byte on the target drive including all files, the slack space, Master File Table, and metadata in exactly the order they appear on the original. Whereas casual users make copies of files when their machines are running, analysts generally create bitstream copies using special software after the computer has been powered down. The bitstream copy can then be saved as a “read only” file so that analysis of the copy will not alter it.

Accordingly, officers conducting analysis at the physical level may be unable to determine exactly how the files and folder appear on a “virtual” level. This distinction is critical to developing the appropriate analogue to real-world searches and thereby appropriately applying the Fourth Amendment.

31 Id. at 332; see also McLain, supra note 25, at 1092–96 (explaining the difference between manual and forensic searches).
32 Kerr, supra note 3, at 541 (internal citations omitted).
33 Id. at 544; see generally, Orin S. Kerr, The Problem of Perspective in Internet Law, 91 Geo. L.J. 357 (2003). But see People v. Emerson, 766 N.Y.S.2d 482, 492 (Sup. Ct. 2003) (claiming that it is impossible to “access any individual image file without going through the folder directory or table of contents page”).
II. DETERMINING AGENTS OF THE GOVERNMENT: AGENCY PROBLEMS IN THE CYBERCRIME CONTEXT

The unique nature of computer storage, both in terms of size and format, creates problems that the traditional doctrine of agency is ill-equipped to handle. This Part describes the facts of several cases that highlight these problems and the approaches developed by various courts. These real-world cases also serve as a basis for the analysis developed in Part IV.

One of the most common factual situations giving rise to private search analysis in computer cases involves repair technicians who observe evidence of illegal activity—usually child pornography—while attempting to fix a client’s computer. United States v. Barth provides a good example of the repair problem, as well as a factual twist raising further agency issues.

Michael Barth, a self-employed accountant, voluntarily turned over his computer to a repairman, Ken Kellar, because it was running slowly. Kellar, while attempting to diagnose and solve the problem, opened a .jpg file that contained an image of what appeared to be child pornography. He immediately shut down the computer and contacted law enforcement. Interestingly, Kellar was an FBI confidential informant, and, while waiting for a return call...

---

See, e.g., United States v. Grimes, 244 F.3d 375 (5th Cir. 2001); United States v. Barth, 26 F. Supp. 2d 929 (W.D. Tex. 1998); Emerson, 766 N.Y.S.2d at 482; see also DOJ 2009 Manual, supra note 13, at 11 (noting that repair technicians finding child pornography is a “common scenario”).


See id. at 932–35 for the facts in this case, which will not be cited separately here.

".jpg" is a file extension commonly associated with photographic images. Kerr, supra note 3, at 544 n.57.

The opinion does not provide any information as to the file name of the image, implying that Kellar opened it as a normal part of his diagnosis.

Because of FBI policy at the time, this fact was unknown to the other law enforcement officers (including FBI agents) and the Assistant United States Attorney ("AUSA"), who advised and directed the subsequent investigation. Believing that this hampered the ability of the investigators and the AUSA to make informed legal judgments about the case, the judge refused to apply the “good faith” exception to the otherwise impermissible search and attached a postscript to the opinion “urging the FBI to review its policy on confidential informants like Kellar . . . .” Barth, 26 F. Supp. 2d at 942–43. See also Stephan K. Bayens, The Search and Seizure of Computers: Are We Sacrificing Personal Privacy for the Advancement of Technology?, 48 Drake L. Rev. 239, 256 (2000) ("[I]t is no surprise that private computer technicians are rapidly becoming confidential informants for various law enforcement agencies. Due to the
from his FBI contact, he alerted the Odessa Police Department (“OPD”), to whom he had also previously provided information.\footnote{The Court does not indicate the nature of Kellar’s prior assistance to either the FBI or OPD.} OPD Officer Roy Vic asked Kellar to bring in the hard drive the following day, and FBI Special Agent Jane Kelly instructed him to copy all of the files onto removable disks so that an agent could pick them up the next morning. Kellar indicated that he would take the computer to the OPD offices to make copies, and Agent Kelly concurred with his decision. After his conversations with the FBI and OPD officers, Kellar restarted the computer, opened additional files, and discovered more seemingly illicit images. He took the computer to OPD the next day and, after Kellar and OPD officers reviewed some of the files on it, allowed OPD to make a copy of the hard drive. Eventually a search warrant was obtained, based solely on the information provided by Kellar. In the subsequent prosecution, Barth challenged the evidence as the fruit of impermissible warrantless searches, arguing, inter alia, that Kellar was a government agent and that law enforcement had impermissibly expanded the scope of Kellar’s search.\footnote{Barth, 26 F. Supp. 2d at 935.}

Addressing the agency issue, the court held that although Kellar’s status as a confidential informant was potentially problematic, it did not necessarily make him a government agent because there was “no evidence that Kellar intended to assist law enforcement officers when he initially viewed the image.”\footnote{Id. at 936.} But the court found the subsequent private search “[m]ore troublesome” because Kellar “was not opening private files in an effort to repair the machine; he did so for the purpose of assisting law enforcement officials.”\footnote{Id.} This, the court held, made Kellar an agent of the government, even though no law enforcement official directed or even expected him to conduct that search.\footnote{Id.} Because Kellar had discussed the case with an FBI agent, the court held that the government was on notice of
the likelihood of a private search, which “triggered the acquiescence.”

Agency issues also arise when individuals “hack” into another’s computer and then turn over files discovered on that computer to law enforcement. As discussed above, the private search exception has no exclusionary rule or statutory suppression remedy, even for otherwise illegal activity. Normally, then, evidence obtained from an illegally-accessed computer is admissible against a defendant, assuming, of course, that the intruder was working independently of the government.

In United States v. Jarrett, an individual using the name “Unknownuser” employed a “Trojan horse” to gain unauthorized access to the defendant’s computer, a tactic he had used previously against another individual who was subsequently convicted of sexual exploitation of minors. While browsing the defendant’s files, he found several images of child pornography, which he then forwarded to law enforcement officials. In the course of several e-mail exchanges between law enforcement and Unknownuser about the cases, FBI Agent Margaret Faulkner wrote Unknownuser in what the court described as “the proverbial ‘wink and a nod’”:

---

45 Id.
46 See supra note 11 and accompanying text.
47 This raises the disturbing possibility of significant abuse. If one is able to access another’s computer and retrieve files, she could likely plant files on the victim computer as well. Thus, one could “hack” into a computer, add images of child pornography, and then send some of those files to law enforcement to cause an arrest of the unwitting victim. Depending on the skill of the intruder, such a scheme would be very difficult, if not impossible, to detect. See, e.g., Jordan Robertson, AP IMPACT: Framed for Child Porn—By a PC Virus, ABC News, Nov. 8, 2009, http://abcnews.go.com/Technology/wireStory?id=9028516.
48 338 F.3d 339 (4th Cir. 2003).
49 A “Trojan horse” is a program willingly installed by a user but that contains a hidden malicious element. See, e.g., United States v. Kline, 112 F. App’x 562, 564 n.1 (9th Cir. 2004) (“[The private searcher] attached his ‘Trojan Horse’ virus to pictures of child pornography on the internet. When an individual downloads a picture, as [the defendant] did, the virus is also downloaded onto that individual’s computer. The virus then allows [the private searcher] to open, alter, and download files on the infected computer.”).
50 See Jarrett, 338 F.3d at 341 (citing United States v. Steiger, 318 F.3d 1039, 1044 (11th Cir. 2003)). The court assumed, as does this Note, that Unknownuser is male, and thus referred to “he” and “his.”
51 Id. at 342.
I can not ask you to search out cases such as the ones you have sent to us. That would make you an agent of the Federal Government . . . . But if you should happen across such pictures . . . please feel free to send them to us . . . . We also have no desire to charge you with hacking.\textsuperscript{52}

The court, though acknowledging that “the Government operated close to the line in this case,” held that the evidence against Jarrett was admissible because the “wink and a nod” e-mails were almost all sent after the search of Jarrett’s computer had already occurred.\textsuperscript{53} Unknownuser’s previous contacts were not enough to establish an “ongoing relationship” with law enforcement, and evidence from his subsequent searches was therefore admissible. The court indicated, though, that further evidence developed by Unknownuser would be inadmissible.\textsuperscript{54}

Though complicated slightly by technology, most agency questions arising from repair technician and virtual-intruder situations are amenable to this type of traditional private search exception analysis.\textsuperscript{55} But cybercrime can present more difficult complications in other contexts. For example, several states have enacted laws mandating the reporting of illegal material found during a private search.\textsuperscript{56} Some specifically require computer repair technicians to report any potentially illegal material they find while examining a computer, with stiff penalties for non-reporting.\textsuperscript{57}

\textsuperscript{52} Id. at 343.
\textsuperscript{53} Id. at 347.
\textsuperscript{54} Id. at 346–47 (noting that “more explicit representations and assurances (as in the post-hoc Faulkner emails)” would be needed to show an agency relationship).
\textsuperscript{55} The Jarrett court, for example, applied the test established by \textit{Skinner v. Railway Labor Executives’ Ass’n}, 489 U.S. 602, 614 (1989) (regarding drug tests of railway employees), and its progeny. 338 F.3d at 344.
\textsuperscript{56} See Child Welfare Information Gateway, Mandatory Reporters of Child Abuse and Neglect: State Statutes Series 3 (2008), www.childwelfare.gov/systemwide/laws_policies/statutes/manda.pdf (“In approximately 18 States and Puerto Rico, any person who suspects child abuse or neglect is required to report. Of these 18 States, 16 States and Puerto Rico specify certain professionals who must report but also require all persons to report suspected abuse or neglect, regardless of profession.”).
\textsuperscript{57} See National Conference of State Legislatures, Child Pornography Reporting Requirements (ISPs and IT Workers) (2008), http://www.ncsl.org/default.aspx?tabid=13460 (noting at least seven states that mandate reporting of child pornography by computer technicians, the majority of which provide criminal penalties for failure to report).
United States v. Peterson addressed just such a statute.\(^{58}\) Harry Peterson took his computer to a local repair center because of boot errors.\(^{59}\) Harry Griffin, the technician on duty, attempted to fix the problem. Once he was able to power up the computer, he noticed “several adult links to web sites” with titles such as “Lolitas Live.” Griffin continued to diagnose the boot error and, while doing so, explored the “My Documents” folder, finding files with male names. He opened one of the files and discovered what appeared to be child pornography. “[R]emember[ing] news stories that reported computer stores were required by law to report ‘evidence of child pornography to the Police[,]’ [h]e . . . decided to ‘investigate’ a little deeper” and “opened several files under the ‘My Documents’ section that revealed” apparent child pornography.\(^{60}\) He also found pornographic video clips but could not determine if the participants were underage.\(^{61}\) Griffin copied some of the files to provide to the police because he was “unsure of what to do next.”\(^{62}\)

The South Carolina law Griffin remembered provides that “any computer technician working with a computer who views an image of a child . . . engaging in sexual conduct . . . must report the name and address of the . . . owner or person in possession of the computer to law enforcement officials.”\(^{63}\) Unlike similar laws in other states,\(^{64}\) it does not apply criminal sanctions to a failure to report but does insulate “anyone making the report” from civil liability.\(^{65}\)

The court held that Griffin was not an agent of the government for Fourth Amendment purposes, writing that “[i]t cannot be said that the language of this statute shows that the government knew of and acquiesced in Griffin’s search.”\(^{66}\) Based on this determination, it did not consider whether Griffin’s search was intended to assist law enforcement.\(^{67}\)

---

\(^{58}\) 294 F. Supp. 2d 797 (D.S.C. 2003), aff’d, 145 F. App’x 820 (4th Cir. 2005).

\(^{59}\) See Peterson, 294 F. Supp. at 799–800 for the facts of this case, which will not be cited separately here.

\(^{60}\) Id. at 800.

\(^{61}\) Id. (“I could not see faces in either clip, so I have no sure idea how old the participants were.”).

\(^{62}\) Id.


\(^{64}\) National Conference of State Legislatures, supra note 57.

\(^{65}\) S.C. Code Ann. § 16-3-850.

\(^{66}\) Peterson, 294 F. Supp. 2d at 805.

\(^{67}\) Id.
A further agency wrinkle develops for non-law enforcement government agents. Computer administrators employed by the government—for example, a state university network administrator or employees of a government agency’s IT department—generally have near-total access to the files of users on their networks and take steps, including searching those private files, to protect the security of the network. Are the fruits of those searches then admissible against a defendant?

The case of United States v. Heckenkamp provides some preliminary answers. Jeffrey Savoy, a computer network investigator for the University of Wisconsin-Madison—a public school—was alerted by FBI Special Agent Terry Rankhorn to possible unauthorized access of the school’s system. Savoy investigated the problems and discovered that an unauthorized individual had gained root-level access, creating the potential for substantial disruption to the system. In an attempt to protect the university network, Savoy searched the defendant’s computer remotely. He then re-contacted Agent Rankhorn, who advised Savoy to wait to take further action, as Rankhorn was attempting to obtain a search warrant. Instead, Savoy, accompanied by university police officers, physically entered the defendant’s unoccupied dorm room through an open door and unplugged the defendant’s computer. Officers later obtained consent to search the computer.

---

68 Though the Supreme Court’s decision in New Jersey v. T.L.O., 469 U.S. 325, 333 (1985), established that, in general, public employees other than law enforcement are covered by the Fourth Amendment, the exclusionary rule might not apply to their unauthorized searches. 1 LaFave, supra note 8, § 1.8 ("[T]he T.L.O. case made it abundantly clear that the question of whether the Fourth Amendment is applicable to certain non-police governmental activity and the question of whether the Fourth Amendment’s exclusionary rule is applicable to that conduct are not one and the same and might not inevitably be answered in the same way.").

69 For a discussion of whether computers connected to a university network are truly private, see infra Section IV.B.

70 482 F.3d 1142 (9th Cir. 2007).

71 Id. at 1143. Agent Rankhorn was alerted to a problem by a computer system administrator for Qualcomm Corporation, who had discovered unauthorized access of his company’s network. Agent Rankhorn then traced the information back to the university. Id.

72 Id. at 1145.

73 Id.

74 Id.
The Ninth Circuit examined the case through the lens of Heck-enkamp’s reasonable expectation of privacy and only briefly considered whether Savoy was an agent of the government for Fourth Amendment purposes:

Although Savoy was aware that the FBI was also investigating [potential computer crimes], his actions were not taken for law enforcement purposes. Not only is there no evidence that Savoy was acting at the behest of law enforcement, but also the record indicates that Savoy was acting contrary to law enforcement requests that he delay action.

Under these circumstances, a search warrant was not necessary because Savoy was acting purely within the scope of his role as a system administrator.75

According to this analysis, Savoy was not an agent of the government, despite his status as a government employee and the fact that university police officers accompanied him to the defendant’s room.76

Each of the situations presented above highlights the tension inherent in applying the traditional agency rules to a digital world. Solutions to these problems are examined below in Part IV, but this Note first examines further problems that arise in the second prong of the private search exception: scope.

III. THREE APPROACHES TO SCOPE PROBLEMS IN REENACTED PRIVATE COMPUTER SEARCHES

Thus far, very few courts have addressed the issues that arise when law enforcement reenacts or expands a private computer

75 Id. at 1147.
76 See also 1 LaFave, supra note 8, § 1.8 (“[W]hen the public official is not a police officer, is not otherwise a part of the criminal justice system in the broad sense of that phrase, and does not have responsibilities which involve (except perhaps upon the rarest of occasions) investigation of activities which might later be a proper subject of criminal prosecution or similar proceedings, then it just may be that the prospect of exclusion bringing about any deterrence in like future situations is so remote that the [good faith exception] would properly be applied.”).
search.\textsuperscript{77} Three approaches have emerged from the case law, each employing a different level of generality to determine the appropriate extent of a reenacted search.\textsuperscript{78}

\textbf{A. Limiting the Scope to Files}

The first and most specific approach is exemplified by \textit{United States v. Barth},\textsuperscript{79} the facts of which are discussed above in the context of agency.\textsuperscript{80} To recall, law enforcement officers copied and searched Barth's entire hard drive, though the repair technician who had originally discovered the illicit images had only opened a few files.

The court held, independent of its conclusion that the repair technician was an agent of the government when he viewed all but one of the files, that officers had impermissibly expanded the scope of the private search.\textsuperscript{81} First, it found that Barth retained a reasonable expectation of privacy in the contents of his computer, an expectation that was destroyed only as to the one file the repair technician, Kellar, had viewed as a private actor. Because officers viewed many more images prior to obtaining a warrant, their search “far exceeded Kellar’s viewings.”\textsuperscript{82} Additionally, the taint of this impermissible search extended to the subsequent warrant-based searches, rendering them invalid as well.\textsuperscript{83}

Thus, \textit{Barth} stands for the proposition that government reenactment of a private computer search must be limited to the individual \textit{files} already searched. It held that the rest of the computer,

\begin{itemize}
  \item \textsuperscript{77} See Donald Resseguie, Note, Computer Searches and Seizure, 48 Clev. St. L. Rev. 185, 198 (2000) (noting that “there are but a few reported cases involving private party searches of computers”).
  \item \textsuperscript{78} The three cases presented here serve merely as exemplars of the varying approaches courts have adopted. They are not the only cases to have considered the issue but provide the best starting point for analysis of the positions.
  \item \textsuperscript{79} 26 F. Supp. 2d 929 (W.D. Tex. 1998).
  \item \textsuperscript{80} See supra notes 36–46 and accompanying text.
  \item \textsuperscript{81} \textit{Barth}, 26 F. Supp. 2d at 937.
  \item \textsuperscript{82} Id. The court never indicated how many specific files were searched or how many images of child pornography were found.
  \item \textsuperscript{83} Id. at 938–39. Barth also consented to the search of his home and office but, because he had been informed of the existence of the warrant, the court held that the consent was involuntary. Id. at 940.
\end{itemize}
even files in the same folder as that already searched, was beyond the scope of the private search.\footnote{The Tenth Circuit reached a similar conclusion for warrant-based searches in United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999). In Carey, officers had a warrant to search the defendant’s computer for evidence of drug trafficking. Upon discovering evidence of child pornography, the investigating officer abandoned the search for drug evidence and spent five hours looking for additional child pornography. The court held that the images were “closed files” and thus the officer was “expanding the scope of his search” when he opened additional files. Id. Though the Carey court focused on the “plain view” exception to the warrant requirement, its reasoning closely resembles that of Barth.}

\section*{B. Limiting the Scope to Folders}

A second approach, taken in People v. Emerson, focuses on digital folders rather than files.\footnote{766 N.Y.S.2d 482 (Sup. Ct. 2003). On reargument, the court declined to alter its original decision. Id. at 495.} The facts of Emerson mirror many of the other private search cases. Specifically, Emerson was unable to boot his computer and so voluntarily provided the hard drive to a technician for repair.\footnote{The facts of this case appear in 766 N.Y.S.2d at 484–85 and will not be cited separately here.} The technician, Patrick Mulrooney, examined the computer on December 7. After locating several viruses, Mulrooney was able to reboot the drive. Once the computer started, he immediately found several files with pornographic titles.\footnote{The court does not say that these file names indicated child pornography, however. Id. at 484.} As he continued to work on the computer, Mulrooney opened a folder, labeled “xxx,” and found “pages of file names describing children performing sexual acts.”\footnote{Id.} Mulrooney found similar files in a separate folder, labeled “MPG.”\footnote{Id.} He opened some of these files and found that they too contained child pornography.

Based on these discoveries, Mulrooney contacted the local police department, which sent an officer the following Monday, December 10. Mulrooney opened several of the files containing the child pornography to show the officer, who then took the computer, for which he obtained a search warrant the following day. Emerson argued that Mulrooney, when conducting his private search on December 7, accessed eighteen files in the “xxx” folder...
and six in the “MPG” folder, whereas six “xxx” files and thirty-one “MPG” files were accessed in front of the officer. Thus, Emerson claimed, the government search impermissibly exceeded the private search and the evidence obtained from the expanded search should be suppressed.  

Unlike the Barth court, the Emerson court focused on the computer folders, holding that the folders were “‘closed containers’ as that term has been interpreted under the Fourth Amendment.” The court also attached “critical importance” to the fact that the searched files and folders actually contained child pornography, as their titles had apparently suggested. The court summarized its holding as follows:

[W]hen an earlier, private search opens child pornography image files on a hard drive in identified computer file folders which the private searcher found replete with file titles plainly suggesting images of like kind, defendant retains no reasonable expectation of privacy with respect to additional such image files in the same two computer file folders.

---

90 On reargument, the defendant claimed that the limits of the technical evidence should require the court to assume that the files and folders were searched for the first time on December 10. The court rejected this assumption as “without merit” as the original decision “did not turn upon this particular detail.” Id. at 492.

91 Id. at 487. The court did leave open the possibility of a Barth-type analysis, writing that “perhaps even the individual image files themselves” constituted closed containers, but did not apply this framework, opting instead to focus on folder contents and file names. Id.; cf. Resseguie, supra note 77, at 203 (“When a small computerized address book or pager is compared to a closed container, this makes a great deal of sense since these devices will generally have the ability to store a limited amount of information all of which is similar. When applied to a larger computer storage device, such as a PC hard drive that has the ability to store a vast amount of information of various types, the closed container analogy is limited.”).

92 Emerson, 766 N.Y.S.2d at 487. Despite the importance of these file names to the court’s analysis, the opinion does not provide the name of any file. On reargument, the court attempted to distinguish situations involving “simple obscenity” from child pornography. “If we were only dealing with materials alleged to be obscene . . . [the Court would need to make an] additional finding beyond sexual explicitness, which could only occur by a viewing of the files . . . In the context of child pornography, however, a labeling which clearly says that an image file contains a sexual performance by a child . . . needs no additional viewing to determine that it is, indeed, contraband.” The court is not clear as to what labels clearly and inevitably reveal their contents in such a way. Id. at 493–94.

93 Id. at 488.
Despite some ambiguity, the Emerson decision seems to constrain law enforcement to searches conducted within the same folders, but not the same files, as the private search.\(^{94}\) The court did not, however, decide if files or folders are the correct level of analysis when file names are not “plainly suggest[ive]” of illicit contents.\(^{95}\)

C. “Limiting” the Scope to Disks

A third approach appears in United States v. Runyan.\(^{96}\) In Runyan, the defendant’s estranged wife, Judith, broke into his home and retrieved several computer disks.\(^{97}\) One of Judith’s friends then viewed some of the contents of some of the disks. Upon finding images of child pornography, she contacted the local sheriff’s department and turned over several of the disks. Over the following weeks, Judith provided additional disks to various law enforcement agencies. During the ensuing investigation, Customs Service Special Agent Rick Nuckles asked to participate in the case. He was provided with all the relevant physical evidence, including all of the disks provided by Judith and her friend. He then “performed an analysis on every piece of evidence he had received, copying the materials onto blank CDs.”\(^{98}\) He examined several of the images from each disk, including disks that neither Judith nor her friend had accessed. Based in part on this information, Agent Nuckles filed for two search warrants, one to search all the disks for illicit images and another to search Runyan’s home for any computer devices. One of the affidavits indicated that another officer had

---

\(^{94}\) On reargument, the court likened folders to a “table of contents” and asserted that it is impossible to access a file without accessing the folder first. Id. at 494. But see supra note 33 and accompanying text.

\(^{95}\) Emerson, 766 N.Y.S.2d at 488; see also United States v. Knoll, 16 F.3d 1313, 1320 (2d Cir. 1994) (“If the files were closed and their contents not apparent from the exterior, the reasonable expectation of privacy continued so long as the files had not been searched before contact with the government occurred.”).

\(^{96}\) 275 F.3d 449 (5th Cir. 2001).

\(^{97}\) The court referred to compact discs, 3.5-inch floppy disks, and ZIP disks collectively as “disks.” The facts in this case appear in 275 F.3d at 452–56 and will not be cited separately here.

\(^{98}\) Id. at 454.
conducted a “cursory” review of the disks. Based on this information, a magistrate judge issued both warrants.\(^9^9\)

Like the courts in *Barth* and *Emerson*, the appellate court applied the closed-container analogy to digital storage.\(^1^0^0\) Unlike those courts, however, it regarded the *disks*, rather than files or folders, as the relevant container.\(^1^0^1\) Thus, the court framed the question presented as “whether the police exceeded the scope of the private search when they examined the entire collection of ‘containers’ (i.e., the disks) turned over by the private searchers, rather than confining their search to the selected containers examined by the private searchers.”\(^1^0^2\) The court concluded that

the police exceed the scope of a prior private search when they examine a closed container that was not opened by the private searchers unless the police are already substantially certain of what is inside that container based on the statements of the private searchers, their replication of the private search, and their expertise.\(^1^0^3\)

Applying that rule to the facts before it, the court held that government searches of the disks the wife had searched were acceptable, while searches of disks she had not accessed were not.\(^1^0^4\)

**D. Are the Three Approaches Actually Different?**

In many respects, these approaches employ quite similar analytical methodologies. For example, each court in the cases discussed above employed the “closed-container” analogy\(^1^0^5\) and examined

\(^9^9\) The search of Runyan’s home revealed one additional image of child pornography, on a backup tape.

\(^1^0^0\) Runyan, 275 F.3d at 461.

\(^1^0^1\) Id. at 458 (“Because neither party contests this point, we assume without deciding that computer disks are ‘containers.’”). The court later emphasized that it was “assuming without deciding that the parties are correct in their characterization of computer storage devices as ‘closed containers.’” Id. at 462 n.13. Despite these caveats, the court nowhere indicated that it preferred, or even considered, an alternative analogy.

\(^1^0^2\) Id. at 462.

\(^1^0^3\) Id. at 463.

\(^1^0^4\) Id. at 464.

\(^1^0^5\) Id. at 461; United States v. Barth, 26 F. Supp. 2d 929, 936 (W.D. Tex. 1998); People v. Emerson, 766 N.Y.S.2d 482, 487 (Sup. Ct. 2003) (citing Runyan, 275 F.3d at 464–65).
the defendant’s expectation of privacy in the items examined. Indeed, the Emerson court’s opinion favorably quoted a lengthy section of Runyan, though it expressly limited the approval of that analysis to the Emerson facts.\textsuperscript{106} It also left open the slight possibility that files, rather than folders, may be the proper level of analysis.\textsuperscript{107} Additionally, the courts in both Barth and Runyan ruled in favor of the defendant (at least partially), and the Emerson court seemed willing to do so had the files been named less suggestively.

Two important distinctions, however, divide the approaches. First, and most significantly, each differs as to the application of the closed-container analogy to the digital world: Runyan applies it to disks,\textsuperscript{108} Emerson to folders,\textsuperscript{109} and Barth to files.\textsuperscript{110} As will be seen below, this seemingly small difference has substantial implications. Second, the Emerson and Runyan courts permit law enforcement expansion of a private search if officers are “substantially certain” that the unsearched files contain illicit material;\textsuperscript{111} Barth does not provide such an expansion. Section IV.B examines these distinctions and argues that limiting the scope of the private search to files provides the best framework.

\textsuperscript{106} Emerson, 766 N.Y.S.2d at 489 & n.4 (“This court agrees with the [Runyan] rationale insofar as it applies to the particular facts [here] . . . . Because of the location and labeling of the computer image files in the ‘MPG’ folder in defendant’s hard drive, it is unnecessary to apply the full reach of Runyan’s holding . . . to the facts of this case.”).

\textsuperscript{107} Id. at 487 (“We start with the proposition that the computer folders containing the images of child pornography, and perhaps even the individual image files themselves, are ‘closed containers’ . . . .”).

\textsuperscript{108} 275 F.3d at 458.

\textsuperscript{109} 766 N.Y.S.2d at 487.

\textsuperscript{110} 26 F. Supp. 2d at 937 (“These files should therefore be afforded the full protection of the warrant requirement . . . . The Court also finds that Defendant did not lose his reasonable expectation of privacy in his closed, individual files . . . .”).

\textsuperscript{111} The Runyan court set forth several factors for making this determination, including “statements of the private searchers, their replication of the private search, and their expertise . . . .” 275 F.3d at 463. The Emerson court agreed with this analysis to a limited extent. 766 N.Y.S.2d at 489 n.4.
IV. SELECTING THE BEST APPROACH

A. Broadening the Agency Definition for Cybercrime Cases

As discussed above, courts dealing with the problems of Fourth Amendment agency in the context of cybercrime have taken a variety of approaches. To get the right answers, though, courts must first ask the right questions. The court in United States v. Barth, for example, properly analyzed the influence of the informant’s prior service to law enforcement and the effect of silent acquiescence to further searches. Likewise, the court in United States v. Jarrett provided an extensive discussion of the email exchange between law enforcement and Unknownuser and then correctly noted that, because these communications occurred after the search, they did not create an agency relationship. The court in United States v. Heckenkamp, however, brushed over the fact that Savoy, the computer administrator, was employed by the State, noting only that he “and the other network administrators generally do not have the same type of ‘adversarial relationship’ with the university’s network users as law enforcement officers generally have with criminal suspects.” Such cursory dismissal of an important point obscures the limits of the exception and hinders the ability of future courts to offer more refined analysis.

Instead of merely commenting in passing that Savoy should be treated as a private citizen, the Heckenkamp court should have followed the lead of the courts in Barth and Jarrett by engaging the difficult issues, especially those that form the foundation of later analysis. Specifically, the court should have looked beyond Savoy’s actions in that particular case to his role more generally. His job was to administer and protect the university’s computer network. He no doubt knew that unauthorized access of that network was

112 See supra Part II.
113 26 F. Supp. 2d at 935–36.
114 338 F.3d 339, 347 (4th Cir. 2003).
115 482 F.3d 1142, 1148 (9th Cir. 2007).
116 The court in United States v. Butler, 151 F. Supp. 2d 82, 85 n.2 (D. Me. 2001), recognized the potential agency issues inherent in a search by university officials of a student’s computer records but declined to consider them because it ruled that the defendant had no standing to challenge the search. “I therefore do not address other interesting issues, [such as:] . . . Were the actions of University employees themselves a search because as employees of a state institution they are state actors?”
illegal and that his investigations, though at least initially designed to protect the network, could produce evidence against a defendant, especially as he was originally alerted to the matter by an FBI Special Agent. Further, he apparently had the university police—clearly government actors—at his disposal, as multiple officers accompanied him to his physical search of the defendant’s room.

Acting against the wishes of a government agent does not, by itself, make one a private citizen. For example, if a police captain tells one of her officers to delay a search until a warrant is obtained, but the officer searches anyway, a court would almost certainly hold that the search was done by the government and is therefore not subject to the private search exception. In this case, Savoy was a public official with investigatory duties, who knew that his investigations could lead to prosecutions, and who had law enforcement officers at his disposal when he sought to conduct a physical search. In light of these factors, the reasoning—and probably the result—in Heckenkamp should have proceeded much differently. Heckenkamp’s analysis is entirely premised on the assumption that Savoy is properly treated as a private citizen. Without that assumption, the remaining discussion of his purpose and intent is largely irrelevant. The court not only skipped over this foundational element, it reached the wrong result in doing so.

Expanding the number of individuals treated as private citizens greatly expands the reach of the private search exception. As the class of private actors is expanded, the realm of private information becomes more limited. To protect the purpose of the exception, the presumption should be that any public employee, when performing her government duties, is a government actor. The government would then need to demonstrate why the individual should not be so treated in a particular case. This approach provides at least some disincentive for publicly employed computer administrators, who have near total access to users’ putatively private files, to snoop around, as anything they find might not be usable in a criminal trial. It does not commit the opposite error, however, as the government may still argue that, in any given case, the public official is not properly considered a government actor and

---

117 Heckenkamp, 482 F.3d at 1143.
118 Id. at 1145.
that the suppression remedy would pose no deterrent effect. The case-by-case nature of traditional agency analysis is thereby preserved.

*United States v. Peterson* further reflects the dangers of excessive expansion of the private search exception in computer cases. Holding that mandatory reporting statutes do not create an agency relationship—and that actions taken pursuant to them are therefore outside the scope of the Fourth Amendment’s protections—is problematic for several reasons.

First, such reporting statutes, especially those states that attach criminal penalties to non-reporting, mandate private action—the essence of government coercion. Though no statute imposes an affirmative obligation to conduct additional searches upon discovery of illegal material, this fine distinction is likely to be lost on average citizens seeking to avoid criminal sanctions. Unlike most mandated reporters, including social workers, police officers, and hospital employees, computer technicians are unlikely to have received any training regarding the identification of child abuse or their legal duties. When the government, either directly or indirectly, orders a citizen to search another’s private files, coercion has occurred, and the private search exception should no longer apply.

Second, the result in *Peterson* and similar cases encourages fishing expeditions by private individuals and diminishes individual privacy. Individuals seeking to comply with the law may search through more files than necessary, just to be sure that they do not violate the statute. Individuals without legal training cannot be expected to carefully parse statutes to determine the exact extent of their obligations. Indeed, in *Peterson*, the technician was only vaguely aware of the statute in question and admitted that he conducted additional searches specifically because he believed he had

---

120 See generally Child Welfare Information Gateway, supra note 56.
121 See id. at 2.
122 Cf. United States v. Barth, 26 F. Supp. 2d 929, 936 (W.D. Tex. 1998) (“To draw the line at any later time would give Kellar, untrained in law enforcement and unrestrained by the responsibilities and duties of officers sworn to protect the Constitution, a free reign to violate the protections of the Fourth Amendment while nonetheless working for the Government.”).
a legal obligation to do so. Such a situation could easily become common. For example, a repair technician might be aware that he is to report any child pornography found on a computer; believing that he might have an obligation to open files with sexually suggestive file names, and not wanting to risk criminal penalties if he is wrong, a technician may view very private, yet not illegal, information. This search, done precisely because of government threats, should also fall outside the private search exception.

Reporting statutes essentially attempt to draft private individuals into government service without providing them the training to identify illegal material or to handle evidence. Instead, most of the statutes impose criminal sanctions (including fines and jail time), encouraging additional, unnecessary, and intrusive private searching without the protection of the exclusionary rule.

In considering statutory coercion cases, courts should adopt the two-prong agency test, asking (1) “whether the government knew of and acquiesced in the intrusive conduct” and (2) “whether the private party’s purpose in conducting the search was to assist law enforcement.” The party’s intent, for the second prong, will, of course, depend on the facts of each case. By passing mandatory reporting statutes specifically aimed at computer technicians, the government has demonstrated that it is aware of the possibility of searches taken precisely because of the statute, arguably satisfying the first prong. If the facts demonstrate that the private searcher did indeed undertake additional searching because of the perceived statutory duty, the searcher should be considered a government agent for Fourth Amendment purposes.

Including the third prong adopted by some courts (“whether the government requested the action or offered the private actor a re-

---

123 Peterson, 294 F. Supp. 2d at 800.
124 See, e.g., Okla. Stat. Ann. tit. 21, § 1021.4(b) (2009) (“Any person who violates the provisions of this section, upon conviction, shall be guilty of a misdemeanor and shall be punished by the imposition of a fine not to exceed Five Hundred Dollars ($500.00) or by imprisonment in the county jail not to exceed one (1) year, or both such fine and imprisonment.”).
125 See supra note 15 and accompanying text.
126 Cf. Barth, 26 F. Supp. 2d at 936 (holding that the government’s awareness of the possibility of a search, even if the government did not approve of that search, was sufficient to find an agency relationship).
ward would not defeat the argument that a mandated reporter should be considered a government agent. By passing such statutes, the government certainly seems to encourage, if not explicitly request, searches. It is a small logical leap from mandating reporting of the results of a search to requesting the search in the first place. Moreover, by providing civil immunity for reporting and attaching criminal penalties to non-reporting, the statutes offer a kind of reward—report the results of a search and avoid punishment, or fail to report and risk punishment. Such incentives encourage the kinds of government-sanctioned snooping that the Fourth Amendment is designed to prevent.

Using either the two- or three-prong analysis, courts should hold that mandatory reporting statutes—at least as applied to computer technicians and other private individuals untrained in identification and preservation of evidence—constitute government coercion such that searches pursuant to them do not fit within the private search exception. An agency standard that expands the class of persons fitting the role of government agent protects individual privacy without significant harm to law enforcement investigations.

The Barth court recognized the importance of maintaining a narrow exception to the Fourth Amendment’s generally stringent requirements. It could have easily justified the second round of searches by the repair technician on the ground that law enforcement neither directed him to make the search nor knew that he would. The court correctly held, however, that the government’s knowledge of the possibility of a subsequent search and lack of an explicit warning to the contrary made the government complicit in his searches. This narrow formulation puts the onus on law enforcement to rein in private individuals when possible and eliminates the “proverbial wink and a nod” searches that diminish individual privacy with no risk to the state.

B. Narrowing the Scope of Private Searches

To best protect the purposes of the private search exception, the agency prong should be interpreted expansively; for the same reason, the scope prong should be interpreted narrowly. As discussed

---

127 See, e.g., United States v. Crowley, 285 F.3d 553, 558 (7th Cir. 2002).
128 Barth, 26 F. Supp. 2d at 936.
above, courts have adopted three levels of analysis for scope problems in computer cases: disks (Runyan), folders (Emerson), and files (Barth). Of these, the Barth framework is best.

1. A Disk-Based Approach is Excessively Broad and Premised on Faulty Analogies

Beginning at the highest level of generality, a disk-based, Runyan-style analysis premises its reasoning on a faulty analogy. Specifically, the court claimed that officers would be “disinclined to examine even containers that had already been opened and examined by private parties for fear of coming across important evidence that the private searchers did not happen to see and that would then be subject to suppression.”

Though possibly relevant in the physical world, this rationale is entirely unpersuasive in the virtual realm. The Runyan court’s analogy incorrectly assumed that opening one file may allow officers to inadvertently see the contents of other files. This is simply not the case. Though file names may be visible, the actual contents of individual files are not visible unless opened. No court has recognized a privacy interest in the file names, focusing instead on the contents.

The Runyan court’s application of the “closed-container” analogy presents further problems. The court did not seem to understand, or at least did not discuss, the capacity difference between portable storage disks and hard drives. It held that government examination of the entire contents of a computer disk accessed by
a private individual is merely “examin[ing] these materials more thorough-ly than did the private parties.” 134 This standard is particularly troublesome in the digital context. Under the Runyan approach, a private searcher could open a single file on another’s computer and thereby provide the government legitimate warrantless access to the entire hard drive of data. 135 Likewise, a net-worked computer can contain files from a multitude of individuals; permitting government agents to view all of these files merely because a private searcher opened one is unreasonable. 136 The difference in scope undermines the spirit and intent of the private search exception. 137 Such an act is not merely examining the computer “more thoroughly,” but is instead fishing in entirely uncharted waters. 138

---

134 Id. at 464.
135 In a confusing opinion in United States v. Crist, 627 F. Supp. 2d 575, 586 (M.D. Pa. 2008), Chief Judge Kane accepted the Runyan court’s reasoning but contended that a search of the hard drive of a computer exceeded the private search because “[a] hard drive is not analogous to an individual disk. Rather, a hard drive is comprised of many platters, or magnetic data storage units, mounted together. Each platter, as opposed to the hard drive in its entirety, is analogous to a single disk as discussed in Runyan.” It is not clear how this standard should operate, given that several platters of a hard drive can contain portions of a single file and that determining what data resides on which platter is difficult, time-consuming, and otherwise of no relevance. Furthermore, while users can and do place certain files on certain individual disks (for example, family pictures on one CD, business documents on a separate flash drive), they have neither the ability nor the need to place files on particular hard drive platters.

136 Kerr, supra note 3, at 556 (“A single physical storage device can store the private files of thousands of different users. It would be quite odd if looking at one file on a server meant that the entire server had been searched, and that the police could then analyze everything on the server, perhaps belonging to thousands of different people, without any restriction. Furthermore, a single file on a network may actually be stored in several physical boxes. Some computer storage devices may not be stored in any boxes at all. Over time, it should become increasingly clear that the Fourth Amendment should track the information, not the physical box.”).

137 This would be analogous to allowing officers who have authority for limited purposes to be in a house to search, quickly and comprehensively, every container in the house, even if it was not related to their reason for being in the house. See id. (rejecting Runyan as leading to “unpredictable, unstable, and even disturbing results”).

138 See also Clancy, supra note 3, at 240 (“If a private party opens ‘tax records 2004,’ under Runyan it would seem that the tax records for other years may be opened by government agents and not be labeled a search. This approach is undoubtedly incorrect. Nothing in previous Supreme Court caselaw supports viewing the entire filing cabinet as a container that permits wholesale searches of all the files therein once a private party opens one of them.”).
Finally, the Runyan court asserted that the opening of closed containers does not impermissibly expand a private search if the officers “knew with substantial certainty . . . what they would find inside” because such a search “provides the police with no additional knowledge that they did not already obtain . . . and frustrates no expectation of privacy that has not already been frustrated.”

The court characterized this rule in terms of obviousness:

The guideline that emerges from the above analysis is that . . .
[a] defendant’s expectation of privacy with respect to a container unopened by the private searchers is preserved unless the defendant’s expectation of privacy in the contents of the container has already been frustrated because the contents were rendered obvious by the private search.

This context-based analysis results from a fact pattern in which officers did indeed find what they expected. The contents of a computer file are, of course, “obvious” after an examination of the file confirms an initial hunch; a court will be strongly inclined to use post hoc justifications in such cases. Courts should not assume that expectations will always be confirmed, however, as file names are not necessarily indicative of contents. File names and extensions can be changed to whatever the user desires and need not have any connection to the content of the file itself.

Drawing an analogy to traditional searches, Judge Kozinski correctly argued that:

Forcing police to limit their searches to files that the suspect has labeled in a particular way would be much like saying police may not seize a plastic bag containing a powdery white substance if it is labeled “flour” or “talcum powder.” There is no way to know

---

139 Runyan, 275 F.3d at 463.
140 Id. at 463–64.
141 United States v. Hill, 322 F. Supp. 2d 1081, 1090 (C.D. Cal. 2004) (“‘Computer records are extremely susceptible to tampering, hiding, or destruction, whether deliberate or inadvertent.’ Images can be hidden in all manner of files, even word processing documents and spreadsheets. Criminals will do all they can to conceal contraband, including the simple expedient of changing the names and extensions of files to disguise their content from the casual observer.” (quoting United States v. Hunter, 13 F. Supp. 2d 574, 583 (D. Vt. 1998))), aff’d, 459 F.3d 966 (9th Cir. 2006); see also McLain, supra note 25, at 1095 (“It would seem that the possibility of users changing file extensions, then, is more likely to fool judges than police officers.”).
what is in a file without examining its contents, just as there is no
sure way of separating talcum from cocaine except by testing it.\footnote{Hill, 322 F. Supp. 2d at 1090–91. Judge Kozinski continued: “The ease with which child pornography images can be disguised—whether by renaming sexyteenyboppersxxx.jpg as sundayschoollesson.doc, or something more sophisticated—forecloses defendant’s proposed search methodology [limiting officers to keyword and extension-based searching].” Id.}

Thus, while the name of a computer file or folder may allow one to make assumptions about the contents, it is insufficient to overcome the warrant requirement.\footnote{See Clancy, supra note 3, at 243–44 (“[A]lthough the police may have had a high degree of confidence in what they would find when they opened the container, that confidence should not eliminate the applicability of the Amendment; instead, that confidence goes to the reasonableness of the police’s actions.”).}

\textit{Walter v. United States} provides further support for this point.\footnote{447 U.S. 649 (1980).} In \textit{Walter}, several boxes of projector film “depicting homosexual activities” were mistakenly delivered to a third party company.\footnote{Id. at 651.} Each box of film contained “suggestive drawings” and “explicit descriptions of the contents.”\footnote{Id. at 652.} One employee unsuccessfully attempted to view the film by holding it up to a light source.\footnote{Id.} The FBI eventually seized the film and, without a warrant, viewed the film via a projector.\footnote{Id.} The Court considered whether that viewing merely recreated the private search or was instead an improper expansion of the previous search.\footnote{Id. at 656.}

The Court fractured in its holding,\footnote{Justice Stevens announced the judgment of the Court in an opinion joined by Justice Stewart. Justice Marshall concurred in the judgment. Justice White, joined by Justice Brennan, concurred, but wrote separately because he disagreed with the notion “that the Government subsequently may conduct the same kind of search that private parties have conducted without implicating Fourth Amendment interests.” Id. at 661 (White, J., concurring). Finally, Justice Blackmun, joined by the remaining three Justices, dissented, arguing that “[t]he containers . . . clearly revealed the nature of their contents.” Id. at 663 (Blackmun, J., dissenting).} but in the opinion announcing the judgment of the Court, Justice Stevens wrote that “the private party had not actually viewed the films” and, instead, “[p]rior to the Government screening, one could only draw inferences

142 Hill, 322 F. Supp. 2d at 1090–91. Judge Kozinski continued: “The ease with which child pornography images can be disguised—whether by renaming sexyteenyboppersxxx.jpg as sundayschoollesson.doc, or something more sophisticated—forecloses defendant’s proposed search methodology [limiting officers to keyword and extension-based searching].” Id.

143 See Clancy, supra note 3, at 243–44 (“[A]lthough the police may have had a high degree of confidence in what they would find when they opened the container, that confidence should not eliminate the applicability of the Amendment; instead, that confidence goes to the reasonableness of the police’s actions.”).


145 Id. at 651.

146 Id. at 652.

147 Id.

148 Id.

149 Id. at 656.

150 Justice Stevens announced the judgment of the Court in an opinion joined by Justice Stewart. Justice Marshall concurred in the judgment. Justice White, joined by Justice Brennan, concurred, but wrote separately because he disagreed with the notion “that the Government subsequently may conduct the same kind of search that private parties have conducted without implicating Fourth Amendment interests.” Id. at 661 (White, J., concurring). Finally, Justice Blackmun, joined by the remaining three Justices, dissented, arguing that “[t]he containers . . . clearly revealed the nature of their contents.” Id. at 663 (Blackmun, J., dissenting).
about what was on the films.” 151 Therefore, “[t]he projection of the films was a significant expansion of the search that had been conducted previously by a private party,” and the evidence should be suppressed. 152 Importantly, Stevens argued that “[t]he fact that the labels on the boxes established probable cause to believe the films were obscene clearly cannot excuse the failure to obtain a warrant; for if probable cause dispensed with the necessity of a warrant, one would never be needed.” 153 Labeling and context alone, then, are insufficient to justify a warrantless search. Just as the descriptions on the boxes did not justify a warrantless search in Walter, file and folder names do not justify a warrantless digital search.

2. A Folder-Based Approach is Unworkable and Encourages Gratuitous Searching

The folder-based standard proffered in People v. Emerson presents a better framework than the disk-based approach given in Runyan but still suffers from several flaws. Though the chosen level of generality was not particularly significant to the outcome in Emerson, the rationale used by the court could allow future searches excessive latitude.

As discussed above, 154 not all computer searches are based on the hierarchy of folders as they appear to a user. Sophisticated search techniques examine the “physical level” of the data and may not replicate the “virtual level” generally seen by users. A folder-based analysis thus breaks down on both a virtual and physical approach. On the physical level, the folder structure simply does not appear, rendering any folder-based framework ineffectual. 155 On the virtual level, the Emerson court relied heavily on the suggestive titles of the folder names and the fact that the images not privately searched were named similarly to those that had been. Though such a situation may provide probable cause, it does not justify a warrantless search, absent a separate exception. As Justice White noted in United States v. Jacobsen, “the mere existence of probable cause to believe that a container or package contains contraband

---

151 Id. at 657.
152 Id.
153 Id. at 657 n.10.
154 See supra Section I.B.
155 Kerr, supra note 3, at 544.
plainly cannot justify a warrantless examination of its contents.\textsuperscript{156} That probable cause can, however, lead to a warrant—thereby enabling law enforcement to examine additional files.

Moreover, the court did not discuss the proper result in cases involving subfolders with suggestive titles inside of a folder already privately searched. The reasoning could easily be extended such that officers could search every folder contained within a parent folder on the theory that the subfolders are likely to contain similar files or that the folders are suggestively named.\textsuperscript{157} Unlike the defendant in \textit{Emerson}, not all individuals who store child pornography create suggestive file and folder names. Consequently, the government could argue that officers, relying on their experience and the information from a private searcher, were substantially certain that innocuously named folders such as “My Pictures” were likely to contain illicit material. Indeed, officers can do so with near impunity, for if similar illicit material is found, the court will have a much easier time justifying, albeit post hoc, the search.\textsuperscript{158} If nothing incriminating is found, the defendant has little cause to complain and little chance of obtaining any remedy.\textsuperscript{159} Accordingly, there is almost no deterrent to “fishing expeditions” given an even slightly incriminating parent folder.

\textsuperscript{156} 466 U.S. 109, 129 (1984) (White, J., concurring in part); see also id. at 114 (“Even when government agents may lawfully seize such a package . . . the Fourth Amendment requires that they obtain a warrant before examining the contents of such a package.”); United States v. Ross, 456 U.S. 798, 809–12 (1982).

\textsuperscript{157} On reargument of \textit{People v. Emerson}, the court suggested that because the individual file names were in “plain view” and suggestive of illegal content, officers could search them. Presumably this would apply to subfolder names as well. \textit{People v. Emerson}, 766 N.Y.S.2d 482, 494 (Sup. Ct. 2003).

\textsuperscript{158} See, e.g., Justice Stevens’s dissent in \textit{California v. Acevedo}, accusing the majority opinion of such a post hoc justification in a drug seizure case. 500 U.S. 565, 595 n.9, 599 (1991) (Stevens, J., dissenting).

\textsuperscript{159} There are, of course, remedies other than suppression for violation of Fourth Amendment rights. These remedies are rarely successful, however, as they require overcoming several substantial barriers. See Ronald Jay Allen et al., Criminal Procedure: Investigation and Right to Counsel 729 (2005) (“The typical Fourth Amendment case—say, a gratuitous frisk or car search—does not involve the kind of physical injury or property damage that would translate into significant money damages, even assuming liability can be established. Particularly if the plaintiffs are unsympathetic (as many criminal suspects are), juries may be unwilling to impose liability or to award more than nominal amounts in such cases, making lawsuits seem not worth the trouble . . . . Another major obstacle is doctrinal: the courts have created a variety of immunity doctrines that limit government damages liability.”).
The *Emerson* court lent credence to this fear by seemingly employing such post hoc rationalizations in its analysis. Though noting that the discovery of child pornography images was “not, alone, determinative,” the court put “critical importance” on the fact that only child pornography was found. It has been long established, however, that the results of a search cannot serve as its justification.

3. The Benefits of a File-Based Framework

A file-based standard, as the narrowest and most specific of the possibilities, provides the best framework, both in terms of law and policy. First, a file-based approach is the most consistent with the theory of the private search exception. As discussed above, the exception rests on the premise that once one’s private material has been viewed by another, the expectation that the information will remain private is no longer valid. Thus, whatever the private searcher has seen is fair game for law enforcement. Disk- and folder-based standards both expand the scope of this destroyed expectation to include information merely located (virtually) “near” the information already viewed.

This is inconsistent with the theory underlying the exception. To apply an analogy, exposing the information contained in one computer file does not expose the information in other files any more than opening one suitcase exposes the contents of what is in another nearby suitcase. As Professor Clancy argues, “a computer should be viewed as a physical container with a series of electronic ‘containers’—that is, directories, folders, and files that must be each separately opened. Each separate opening is the examination of a new container.”

---

160 *Emerson*, 766 N.Y.S.2d at 488.
161 Id. at 487. The court went on to note that officers did not access “other types of private information elsewhere on the computer’s hard drive,” as though the lack of further incriminating evidence reduced the intrusiveness of the search. Id. at 488.
162 “[I]f any point is solidly grounded in Fourth Amendment jurisprudence, it is that the police cannot ‘bootstrap’ themselves into probable cause; a search may not be justified by what turns up in that search.” 3 LaFave, supra note 8, at § 7.2(d).
163 See supra notes 7–8 and accompanying text.
164 Clancy, supra note 3, at 240; see also Kerr, supra note 3, at 555 (“If you analogize a computer hard drive to a suitcase, each file is like its own zippered pocket in the
Moreover, incriminating evidence will nearly always derive from the content of individual files, as opposed to the labels (that is, file names) of folders or disks. Accordingly, this level is the most logical place to draw the line of what private information has already been viewed. Any other approach allows the government to examine a much greater amount of content (that is, potential evidence) than the private searcher ever did.

Additionally, a file-based standard still provides law enforcement adequate means to investigate possible crimes discovered by private searchers. Officers need merely replicate the private search and determine if the previously viewed files do provide evidence of a crime. If so, those files are admissible against the defendant. If not, or if officers would prefer to look for more files, they need merely to obtain a search warrant, a routine practice for law enforcement agencies.

At least one commentator argues that even a file-level analysis is too broad, because

[i]f the police perform a simple search from within the operating system, they will only be able to see files, making files the relevant “containers.” If, however, the police use forensic tools, the “containers” become the sectors and clusters (which may or may not make up a complete file) on the storage media.

This argument, while accurately distinguishing physical and virtual searches, is simply not relevant in private search situations. Private searches will almost always use the computer at the virtual suitcase. A computer is like a container that stores thousands of individual containers in the form of discrete files.

165 For example, officers might prefer to examine more files for sentencing purposes, as the amount of contraband possessed may determine or influence the applicable sentence.

166 For example, in United States v. Hall, 142 F.3d 988, 991 (7th Cir. 1998), the defendant took his computer to a repair technician who subsequently discovered child pornography. The technician alerted law enforcement, who did not view any files themselves but instead sought—and received—a search warrant for the computer. The court therefore did not need to make any determinations regarding the scope of the private search and, after quickly establishing that the technician was not an agent of the government, upheld the warrant as valid. Id. at 991–94. But cf. United States v. Harned, No. 98-10227, 1999 U.S. App. LEXIS 11397, at *13–14 (9th Cir. June 2, 1999) (“[P]robable cause for a search warrant may not rest entirely upon the bare conclusion of a computer store employee as to the nature of the photographs.”).

167 McLain, supra note 25, at 1096.
level and are extremely unlikely to use forensic tools to search the computer. In recreating a search, then, officers may not expand the scope of the search beyond files opened by the private searcher but, at the same time, should not be overly constrained by the private searcher’s lack of forensic tools. In other words, because files are the smallest unit of navigation encountered on the virtual level used by private searchers, files should determine the scope of the government agent’s search.

Professor Kerr presents a more nuanced version of this point, suggesting that only what is actually “exposed to human observation” has been searched. Thus, metadata, such as access times and modification history, are generally not part of the private search and may not be viewed by law enforcement absent a warrant or other exception. The file-based approach proposed in this Note would permit searching of the metadata of files previously viewed by the private searcher, even if that searcher did not observe the metadata, because once a private searcher views a file, the defendant’s expectation of privacy in that file is lost. Moreover, distinguishing between parts of the files is impossible on a physical-level search (where metadata is included with the rest of the file information).

Additionally, though it is possible to determine retroactively what files a private searcher has viewed, officers are not necessarily able to know what parts of those files the searcher viewed. For example, a private searcher may open a multi-page document file,

168 Kerr, supra note 3, at 547–48 (“[I]n the case of a search by a private actor, government agents may view only the information viewed by the private actor unless they first obtain a warrant.”).

169 See, e.g., Adam Israel, Note, To Scrub or Not to Scrub: The Ethical Implications of Metadata and Electronic Data Creation, Exchange, and Discovery, 60 Ala. L. Rev. 469, 472–73 (2009) (“Metadata is essentially the history of a document. Every comment, every edit, every iteration of a document is hidden within that document, chronicling its life. . . . The metadata of a typical Microsoft Word document may include: the author’s name and initials; the name of the company or organization where the document was created; the name of the author’s computer; the name of the server or network on which the document was saved; the names of previous document authors; the original text, along with any revisions to the original text; template information; any digital comments made on the document; document versions; and hidden text. Metadata is also produced by Corel WordPerfect and other popular word processing software, Microsoft Excel and PowerPoint, and other similar programs. Furthermore, e-mails also contain metadata.”).
but officers would not necessarily know what parts of the document, if any, the searcher viewed, thus presenting numerous practical difficulties in attempting to re-create the search without impermissibly expanding its scope. To draw a real-world analogy, a private searcher who opened a journal may not have read every single page, though police could, using the private search exception, closely examine each entry. Accordingly, the file-level approach, and not an observation-based analysis, best preserves the purposes of the private search exception without unduly hindering law enforcement.\footnote{170}

In the end, the exceptions to the warrant requirement must be as narrow as possible while still retaining their purpose. Excessive expansion obviates the warrant requirement and leads to unnecessarily intrusive searches that are only justified post hoc. As the Supreme Court has noted, “[t]he exceptions to the rule that a search must rest upon a search warrant have been jealously and carefully drawn.”\footnote{175} A file-based standard retains that tight reading of the exception and should be adopted by courts facing similar issues in the future.

\footnote{170 It is perhaps noteworthy that the distinction between Professor Kerr’s and this Note’s proposed framework is largely moot in most private search cases; both analyses would lead to the same results in all the cases discussed here. As Kerr notes, most cases “involve possession of digital images of child pornography, in which the contraband image is both the file contents and the exposed data. The distinction between files and data collapses in this context . . . .” Kerr, supra note 3, at 556. Kerr further concedes that “[t]he exposure-based approach is critical only when the officer has legitimately viewed part of the file but has no authority to conduct a new search through the rest of it,” a rare situation indeed. Id. at 557. The distinction could be important, however, in certain cases. Metadata information—such as who viewed a document and when—may be vital in determining culpability in insider trading and other white collar crimes, for example.

175 Jones v. United States, 357 U.S. 493, 499 (1958). This rule has been cynically attacked on the grounds that it is not actually employed in practice. See, e.g., Edwin Butterfoss, As Time Goes By: The Elimination of Contemporaneity and Brevity as Factors in Search and Seizure Cases, 21 Harv. C.R.-C.L. L. Rev. 603, 649 (1986) (“The Court no longer adheres to the maxim that a search or seizure is per se unreasonable unless it is supported by a warrant or falls within a jealously and carefully drawn exception to the warrant requirement. Instead, the Court simply evaluates police conduct under a general notion of reasonableness.”).}
IV. CRITICISMS OF THE FILE-BASED FRAMEWORK AND RESPONSES

The standard argued for here—that is, an expansive definition of “government agent” and a narrow scope for re-created private computer searches—seeks to limit the force of the private search exception in computer crime cases. One can level a number of criticisms against such a narrow private search exception. This Part considers several such arguments and offers responses to them.

A. The Proposed Standard Hinders Law Enforcement

One objection to the proposed standard is that narrow exceptions to the warrant requirement hinder police investigation, making it more difficult to find and arrest criminals. Though a narrow exception does put greater burdens on investigators, it does not do so in an excessively onerous manner. First and foremost, even absent this exception, law enforcement is still able to obtain warrants based on probable cause.

Exceptions to the warrant requirement merely describe situations in which evidence obtained without a warrant may still be introduced as evidence at trial. As officers only need probable cause to obtain a warrant, a re-created private search of even a small number of files should suffice. Indeed, though file names alone should not allow officers to expand the scope of the previous search, they can be used to convince a magistrate to issue a warrant. Though obtaining a warrant does require investment of some time and resources, the investment is not great.

172 See, e.g., Sagi Schwartzberg, Note, Hacking the Fourth: How the Gaps in the Law and Fourth Amendment Jurisprudence Leave the Right to Privacy at Risk, 30 U. La Verne L. Rev. 467, 484 (2009) (noting the frustration of hacker groups at the perceived reluctance of law enforcement to pursue child pornography cases discovered by private searchers).

173 See DOJ Manual 2009, supra note 13, at 12 (“Even if courts follow the more restrictive approach [of Barth], the information gleaned from the private search will often provide the probable cause needed to obtain a warrant for a further search.”).

174 Federal law provides an affirmative defense for possession of “less than three images of child pornography.” 18 U.S.C. § 2252A(d)(1) (2006); see also id. § 2252(c)(1) (2006). If a private search turns up just three such images, probable cause for a warrant will almost certainly be met.
Rarely will officers have reason to require an immediate search of the computer such that a delay would be detrimental.\textsuperscript{175} Further, even absent a warrant, other exceptions may permit a proper search. If, for example, officers fear that a suspect will delete the data if he is to reacquire the computer (perhaps if the suspect knows law enforcement has been alerted), the exigent circumstances exception may apply.\textsuperscript{176} Alternatively, the government can invoke the “independent source” or “inevitable discovery” doctrines if officers can demonstrate that they would have found the evidence via other lawful means.\textsuperscript{177} Or, depending on the facts of the case, courts might entertain the idea of a special needs,\textsuperscript{178} automobile, or border search exception.\textsuperscript{179} Officers have numerous tools at their disposal, including obtaining a warrant or applying one of the many exceptions to the warrant requirement. Narrowing the private search exception will not significantly hamper police investigation. As Judge Rosenbaum noted concisely: “This suggestion complicates criminal investigations. So does the [F]ourth [A]mendment.”\textsuperscript{180}

B. Defendants Have No Reasonable Expectation of Privacy in Data Voluntarily Provided to Others

Perhaps the strongest objection to a narrow exception for computers is that defendants who voluntarily turn over their computers to repairpersons or knowingly connect to a monitored network

\textsuperscript{175} See Rosenbaum, supra note 3, at 58 (“Once a computer is seized, there will rarely be an exigent need to search it. This allows time for the government to develop, and a court to review, the scope and methodology of the search.”).

\textsuperscript{176} Id. at 57 (“[I]f immediate access is needed—when exigent circumstances are present—the investigator can demonstrate the need and be granted immediate access.”).

\textsuperscript{177} See, e.g., United States v. Barth, 26 F. Supp. 2d 929, 939 (W.D. Tex. 1998) (declining to hold the doctrines applicable on the presented facts).

\textsuperscript{178} See United States v. Heckenkamp, 482 F. 3d 1142, 1147 (9th Cir. 2007) (“Although we conclude that Heckenkamp had a reasonable expectation of privacy in his personal computer, we conclude that the search of the computer was justified under the ‘special needs’ exception to the warrant requirement.”).


\textsuperscript{180} Rosenbaum, supra note 3, at 57.
have lost their legitimate expectation of privacy in the contents of the computer.\textsuperscript{181} Many Internet Service Providers ("ISPs") (especially those in university and government agency settings) expressly note that use of the network may be monitored. Likewise, repairpersons may need to inspect several files to diagnose and solve the problem(s) ailing a computer.\textsuperscript{182} Knowing this, the argument continues, individuals willingly surrender their interests in the privacy of the contents of their computer as long as it is connected to a monitored network or is in the hands of a technician.\textsuperscript{183}

This argument assumes, however, that one loses the expectation of privacy in all files possibly observed, even those not actually opened. As the Supreme Court held in \textit{United States v. Jacobsen}, the Fourth Amendment applies "only if the authorities use information with respect to which the expectation of privacy has not already been frustrated. In such a case the authorities have not relied on what is in effect a private search, and therefore presumptively violate the Fourth Amendment if they act without a warrant."\textsuperscript{184} The \textit{United States v. Barth} court concluded that the defendant "retained his reasonable expectation of privacy in the files when he gave the hard drive to [the computer technician]."\textsuperscript{185} Likewise, the court in \textit{People v. Emerson} seemed to indicate that the defendant’s reasonable expectation of privacy was lost only once the technician

\begin{footnotes}
\item[181] See generally 1 LaFave, supra note 8, \textsection 1.8(b) ("[W]hen one subjects her property to the joint or exclusive control of another, she has thereby assumed the risk that the other person will turn that property over to the police and will allow the police to examine it further."); Clancy, supra note 3, at 220–27 (discussing cases analyzing the expectation of privacy in networked computers).
\item[182] See, e.g., United States v. Caron, No. 03-79-P-H, 2004 U.S. Dist. LEXIS 3663, at *2–3 (D. Me. Mar. 9, 2004) ("Jarvis [the repair technician] followed his usual procedure, which is to start the computer and try to get it to do what the customer is complaining about. When the problem is locking or freezing, Jarvis always goes first to the My Documents and My Pictures files in order to load up and stress the system."). The "My Documents" and "My Pictures" folders are common places to store documents, pictures, and files that the owner may nevertheless wish would remain private.
\item[183] The defendant in \textit{Emerson} seemed to recognize that the technician might find contraband, allegedly telling him, "you're going to see weird things on the D drive because my brother-in-law has a sick sense of humor." People v. Emerson, 766 N.Y.S.2d 482, 484 (Sup. Ct. 2003).
\item[185] 26 F. Supp. 2d 929, 937 (W.D. Tex. 1998).
\end{footnotes}
opened the folders containing the incriminating evidence, not merely when he received the computer from the defendant.\textsuperscript{186}

In the file-based analysis proposed here, the defendant has not lost a reasonable expectation of privacy in unopened files. In other words, though one might not know exactly which files will be searched during the repair process, he or she should not lose privacy interests in the entire hard drive. The private search exception is premised on the idea that items searched by a third party are no longer private. The mere possibility of discovery should not invalidate this expectation.\textsuperscript{187}

Additionally, the validity of monitored network agreements becomes more problematic in, for example, university settings. In such a case, a student in the dormitory, who uses the network for both personal and educational purposes, is forbidden (often both physically and by contractual agreement) to contract with a private ISP to provide unmonitored access.\textsuperscript{188} Thus, the user seemingly must sacrifice the expectation of privacy in all her computer files in exchange for the ability to connect to the university’s monopolistic system. Allowing public university employees to search, for any reason or no reason, a student’s putatively private files and turn over the results to law enforcement eviscerates the protections granted by the Fourth Amendment and once again allows the exception to swallow the rule.\textsuperscript{189}

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{186} 766 N.Y.S.2d at 487. See also State \textit{v. Bellar}, 217 P.3d 1094, 1099 n.5, 1108–09 (Or. Ct. App. 2009), where both the majority and dissent assume without deciding that, at least for state law purposes, a defendant may maintain a privacy interest in his computer even when he gives it to a third party.
\item \textsuperscript{187} Cf. Rosenbaum, supra note 3, at 58 (“[P]lain view should not be equated with the mere fact that the material exists on the same hard drive. A bank robber’s computer may catalogue get-away paths, but this does not justify a disc-wide general search. The [F]ourth [A]mendment requires specificity.”).
\item \textsuperscript{189} See Clancy, supra note 3, at 222–24 (discussing cases considering government employees’ reasonable expectations of privacy in work computers). Compare United States \textit{v. Heckenkamp}, 482 F.3d 1142, 1147 (9th Cir. 2007) (holding that a student had a reasonable expectation of privacy on the network because no university policy announced otherwise), with United States \textit{v. Angevine}, 281 F.3d 1130, 1134 (10th Cir. 2002) (ruling that a government employee had no reasonable expectation of privacy)
\end{itemize}
\end{footnotesize}
here restores the balance by permitting officials to monitor the network and, if necessary, obtain a warrant for specific machines or files, while simultaneously protecting the privacy interests of the system’s users.

C. A Narrow Approach Actually Reduces Privacy

Finally, one could object that a limited exception provides an incentive for private searchers to examine as many files as possible so that a re-enactment of the search by law enforcement will find sufficient evidence of criminal activity to justify an arrest of the suspect. This argument is unavailing for several reasons.

First, the rule is unlikely to create more private searchers or more extensive private searches. Most people who stumble upon contraband on a computer are unlikely to know, understand, or care about the evidentiary rules that apply in court. Accordingly, incentivizing more extensive private searches is unlikely. Similarly, such a rule is unlikely to produce more private snoopers, as those who intrude virtually will do so independently of an evidentiary rule; likewise, those who merely fix computers must wait for one to come to them.

Second, to the extent that this approach does result in increased private searches, this is preferable to greatly expanding the search power of the government. That is, a broader exception merely shifts the search from a private searcher to the government. So, adopting a disk-based, Runyan-type analysis, the viewing of a single file by a private searcher would then allow law enforcement officials, with experts, resources, and time at their disposal to conduct an exhaustive search of the suspect’s computer. The exceedingly intrusive nature of this search, combined with the fact that the government now holds the information, makes this result less desirable than an individual merely perusing files at the “virtual” level.

because of an agency policy of monitoring network traffic), and United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (same). The employee search cases are distinguishable from at least some public university student cases, in that students living in the university-provided dorms connect to the network from their home, the most protected area in Fourth Amendment jurisprudence. Employees are not similarly hindered.
CONCLUSION

The drafters of the Fourth Amendment certainly could not have envisioned the world of computing or the ability to store, search, and quickly retrieve vast amounts of information. Courts have created some exceptions, and expanded others, in an attempt to keep the spirit of the Amendment alive in modern society. Occasionally, however, the expansion of exceptions goes too far. As demonstrated in this Note, courts and commentators have struggled to apply physical world analogies to virtual realities, often coming up short.

To keep the Fourth Amendment relevant, one should keep in mind its spirit and purpose. Fearing an overly zealous and intrusive state, the Framers forced law enforcement to obtain the approval of a neutral and detached magistrate before searching the person, papers, or effects of a citizen. Several exceptions to this requirement have since sprung up, and rightly so. However, they must remain “jealously and carefully drawn” or else risk swallowing the rule and making the warrant requirement irrelevant. The private search exception is based on the premise that the Fourth Amendment only constrains government action and that information viewed by another party is no longer private. Courts should interpret this formulation strictly, as in United States v. Barth, not allowing a private search of one computer file to permit a governmental search of thousands of files on the premise of “re-creating” the private search.

Exceptions to the warrant requirement are just that: exceptions. If officers have probable cause for believing a suspect has committed a crime, they can and should obtain a warrant and search under the aegis of a constitutionally protected power. The warrant requirement is designed to make police work less efficient and is a vital protection citizens have against an oppressive state. Limiting the private search exception in computer crime cases effectively protects the individual while still allowing the government to investigate and prosecute crime.