



The Plain View Doctrine And Computer Searches

Balancing Law Enforcement's Investigatory Needs With Privacy Rights in the Digital Age

The police suspected Montgomery Gray of hacking into the National Library of Medicine's (NLM) computer system at the National Institute of Health. They obtained a warrant to search his computer for NLM documents and "hacker" materials, including certain computer source code. Following departmental computer search protocol, the searching agent methodically opened each and every file on Gray's computer, including image files in a directory titled "Teen." Within this folder, the agent found numerous images of child pornography, leading him to secure a second warrant authorizing a search for child pornography. In Gray's subsequent prosecution for possession of child pornography, the court denied Gray's motion to suppress the images, holding that (1) pursuant to the original warrant, the agent was entitled to examine *all* the files in the computer to determine whether they contained items falling within the scope of that warrant, and (2) based upon this broad authority, the agent could then seize the

pornographic images under the plain view exception to the Fourth Amendment's warrant requirement.¹

Such wide-ranging computer searches have also affected third parties suspected of no criminal wrongdoing whatsoever. For example, in 2004, in a widely publicized case, *United States v. Comprehensive Drug Testing*, the government obtained a warrant to search for and seize the medical testing records of 10 Major League Baseball players suspected of testing positive for illegal steroids.² With this warrant, agents seized the records not only of the players listed in the warrant, but also those relating to hundreds of baseball players and other professional athletes not suspected of any wrongdoing.³ The government justified its actions by claiming that the records of the other athletes were in "plain view," leading the district judge to ask: "What happened to the Fourth Amendment?"⁴

Criminal defense lawyers dealing with document-intensive cases have been asking themselves that same question. The cases described above illustrate the tension in electronic data cases between law enforcement's legitimate need to collect and examine evidence, on the one hand, and parties' Fourth Amendment rights, on the other. As a result of the increasing prevalence of computers in our lives, electronic information is undoubtedly an important source of evidence in many criminal cases. And computers' immense storage capacities present particular challenges for law enforcement, the courts, prosecutors, and defense attorneys when attempting to craft appropriate search protocols. An investigator searching a suspect's computer may encounter intermingled documents, hidden or deleted files, technical problems, password protections, encrypted data, and myriad other challenges.⁵ Often the government cites these particular

BY DAVID H. ANGELI, CHRISTINA SCHUCK, AND AVALYN TAYLOR

challenges to justify requests for wholesale seizure and broad, sweeping searches of digital storage devices, because if inculpatory materials exist, they are most likely intermingled with irrelevant and private documents.

Although courts have historically paid lip service to the notion that challenges associated with computer searches do not justify issuing the government "a blank check,"⁶ every computer search runs the risk of becoming a general, exploratory search. As illustrated by cases like *Gray* and *Comprehensive Drug Testing*, the coupling of the already intrusive, invasive power of computer searches with the plain view exception to the Fourth Amendment's warrant requirement presents a somewhat unique risk of unwarranted invasions into individual and corporate privacy rights. Thus, all parties involved — courts, prosecutors, investigators and defense attorneys — must remain vigilant to guard against the possibility of computer searches becoming an excuse to engage in the "general exploratory search[es]"⁷ the Framers so despised.

This article begins with a brief history of the Fourth Amendment and the courts' universal rejection of general search warrants. Part II addresses the specific challenges and risks that computer searches present to both law enforcement and defendants, particularly in light of the plain view doctrine and the courts' typical application of that doctrine in the context of digital evidence. Part III begins by summarizing the Ninth Circuit's landmark decision in the *Comprehensive Drug Testing* (CDT) case, followed by a discussion of several recent cases in which courts have disagreed with, or refused to apply, the Ninth Circuit's holding in CDT. The article concludes by arguing that the plain view exception should not apply at all with respect to searches of digital content.

I. The Fourth Amendment Prohibits General Warrants

The Framers crafted the Fourth Amendment in response to the loathed and feared general warrants and writs of assistance that the British had so frequently used during colonial times.⁸ General warrants allowed sweeping, exploratory searches of homes for evidence of seditious libel.⁹ With a writ of assistance, a specialized form of a general warrant, officers of the Crown could "go into any house, shop, warehouse, etc.; break open doors, chests, packages

... and remove any prohibited or uncustomed goods or merchandise."¹⁰ Colonists viewed writs of assistance as especially dangerous because they functioned as a "continuous license and authority during the whole lifetime of the reigning sovereign."¹¹

In 1761, John Adams listened to James Otis argue on behalf of 63 Boston merchants petitioning a court in opposition to granting new writs of assistance, and later wrote, "Mr. Otis's oration against the Writs of Assistance breathed into this nation the breath of life. ... [E]very man of a crowded audience appeared to me to go away, as I did, ready to take arms against Writs of Assistance."¹² Indeed, this sentiment led many individual states specifically to outlaw general warrants in their constitutions.¹³

Ultimately, the Framers prohibited general warrants in the Fourth Amendment by protecting citizens against "unreasonable searches and seizures" and requiring a warrant to "particularly describe the place to be searched and the persons or things to be seized."¹⁴ This clause, referred to as the "particularity requirement," requires that "the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit."¹⁵

II. Risk of Computer Searches Becoming Unlawful General Searches

A. Computer Usage and Data

Computers and external electronic storage devices contain an almost incomprehensible amount and variety of data. People and businesses use computers ubiquitously as diaries, photo albums, stereos, telephones, file cabinets, and televisions.¹⁶ In addition to the data stored on a computer's internal hard drive, individuals also save data to external storage devices such as CDs, DVDs, thumb drives, and external hard drives.¹⁷

At its most basic level, electronic data "is simply a collection of ones and zeros"¹⁸ requiring a machine and programs to organize it into something meaningful.¹⁹ Strings of ones and zeros are organized into groups called sectors. Sectors are organized into clusters, which can then be used by software programs.²⁰

A computer file, such as a Microsoft Word document, spans multiple clusters, which the computer's operating system (Windows, MAC OS, or LINUX, for example) tracks on several levels.²¹ First, the computer labels the cluster as

either already used to store data or as available to store data. Thus, and importantly for investigative purposes, a file that has been "deleted" by a computer user is not actually removed from the computer. Instead, the clusters are simply redesignated as available to store data. If the cluster is not "overwritten," the data it holds is recoverable using forensic software. Second, the operating system tracks the location — the file name and folder — in which the cluster is located.

In addition, when a computer user creates a new item, e.g., a letter using Microsoft Word, the computer saves more than just the content typed in by the user. It also saves information called "metadata," which is not immediately visible to the user and which includes information about when the file was created, edited, and accessed.²² Operating systems and applications record information such as Internet usage, when and for how long flash drives were attached, and the times during which the computer was in use. Obviously, law enforcement may be keenly interested in all of that type of data.

B. Methods of Searching Electronic Storage Devices

These vast amounts and varieties of electronic data present unique challenges to law enforcement. The simplest — albeit most time-consuming — way to search a computer is to conduct a manual file-by-file search, whereby an officer simply turns on the computer and begins browsing through all of the files on that computer.²³ This type of search often proves inefficient, incomplete, and even destructive. Considering the immense storage capacities of computers, opening each file within a computer's hard drive or on an external storage device consumes a great deal of time, while leaving a considerable amount of data undetected. Furthermore, during a manual search, an officer cannot access deleted or temporary files.²⁴ This method also risks altering or damaging evidence; for example, merely opening a Microsoft Word document overwrites certain metadata associated with the file.²⁵ Additionally, the simple act of using an operating system creates certain temporary files, possibly overwriting certain clusters previously reassigned from a deleted file.²⁶

For those reasons, it is often much more beneficial for law enforcement to search electronic storage devices using forensic software. Forensic software circumvents the computer's operating sys-

tems and enables law enforcement to access more data and to search more efficiently for evidence.²⁷ For example, the "EnCase" software allows investigators to view data clusters from deleted files not yet reassigned, to search file headers that indicate the type of file associated with the header (regardless of the file extension assigned by the user),²⁸ and to search exhaustively through known text files for particular words or phrases while accounting for misspellings.²⁹

Regardless of the search method employed, an officer typically first creates a bitstream copy, or "mirror image" of the original storage device in a "read only" file.³⁰ This copy duplicates every bit and byte on the target drive, including metadata, deleted files and empty space exactly as it appears on the original.³¹ Because of the time-consuming and technical nature of the two-part search (the imaging portion and the examination portion), law enforcement often requests permission to seize the entire electronic storage device in order to conduct the search in a controlled, laboratory setting.³²

C. Wholesale Seizure of Electronic Data: Fourth Amendment Concerns and Judicial Reaction

In light of these concerns, courts routinely approve and uphold blanket seizures of electronic media, or what the Ninth Circuit has called "seiz[ing] the haystack to look for the needle,"³³ as long as the affidavit supporting the warrant reasonably explains why such a seizure is necessary.³⁴ To satisfy that requirement, officers often explain the complexities of computer searches and how computer users can disguise files with misleading names and false extensions, and encrypt or even "booby-trap" data.³⁵

The customary approval of blanket seizures implicates two particular Fourth Amendment concerns. First, by virtue of the immense volume of data a computer holds and the wide range of uses to which individuals and businesses put those computers, a court authorizing a blanket seizure almost assuredly sanctions the seizure of a large amount of data that falls completely outside the substantive scope of the warrant.³⁶ This effectively turns on its head the traditional sequence of search, followed by selective seizure.³⁷

Second, searching such a vast amount of data and intermingled documents raises the possibility of law enforcement conducting a general search for evidence of any type of illegal

activity, whether or not such activity relates to the allegations and evidence supporting the warrant application. In other words, searches of this type create a significant risk of the "kind of investigatory dragnet that the Fourth Amendment was designed to prevent."³⁸

Some courts have addressed these concerns by implementing safeguards based on the "intermingled documents" rule that has historically applied in the traditional paper document context.³⁹ In *United States v. Tamura*, the FBI executed a warrant authorizing the seizure of corporate documents related to an alleged bribery scheme. When the employees refused to assist the FBI in locating the relevant documents, the agents seized multiple cardboard boxes and dozens of file drawers filled with large quantities of intermingled and unrelated documents, through which agents later sifted in a separate location to find the relevant documents.⁴⁰

Although the court found no reason to suppress any properly seized material, it took special care to establish safeguards and a protocol for searches involving intermingled documents that may have no relevance to the subject of the search. First, the court required the officers to seal or hold the documents pending approval by a magistrate judge, who would monitor the sorting of the documents.⁴¹ Second, the court instructed that when the need for seizing intermingled documents is known beforehand, the affidavit supporting the warrant application should explain why on-site sorting is impractical.⁴² That type of information increases a court's confidence that "the magistrate judge was well aware of what he was authorizing and that the agents knew the bounds of their authority in executing the search."⁴³

Following the *Tamura* opinion, attorney Raphael Winick wrote an influential law review article arguing that computer searches, given their unique nature, should be afforded the same protections as searches involving intermingled documents.⁴⁴ The Tenth Circuit, in *dicta*, quoted from Winick's article in *United States v. Carey*,⁴⁵ and urged law enforcement to employ the *Tamura* safeguards to electronic data that could not feasibly be sorted on-site. In that case, the officer searching Carey's computer for evidence related to drug dealing instead found an image of child pornography.⁴⁶ Abandoning his search for evidence of drug activity, the officer spent five hours deliberately searching for additional evidence of child pornography without applying for a separate war-

rant for that purpose. The government attempted, unsuccessfully, to justify this warrantless search by citing the plain view exception.⁴⁷

Carey illustrates the dangers inherent in wholesale seizures of intermingled files. In this relatively common situation, law enforcement suddenly gains access to countless unrelated, private and even privileged files that are clearly outside the scope of the warrant. As the *Carey* court recognized, the plain view doctrine with the inherently invasive nature of a computer seizure and search presents a grave danger to private parties' Fourth Amendment rights.

Although the U.S. Supreme Court has instructed that "the plain view doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges,"⁴⁸ electronic information seized under that exception has been used in numerous ways: as evidence of other crimes;⁴⁹ to procure additional search warrants;⁵⁰ and to implicate third parties.⁵¹ Those uses call into question whether the application of the plain view doctrine in the context of electronic data can be reconciled with the Fourth Amendment's prohibition of general searches.⁵²

III. Applying the Plain View Doctrine to the Computer Context

The plain view doctrine operates as an exception to the Fourth Amendment's warrant requirement, allowing an officer to seize and/or use evidence outside of the scope of the warrant if (1) the officer was lawfully in the place where the object was seen; (2) the object was in plain view; (3) the object's incriminating nature was immediately apparent, meaning the officer had probable cause to believe the object was contraband or evidence of a crime;⁵³ and (4) the officer had a lawful right of access to the object itself.⁵⁴ The initial application of the plain view doctrine contemplated a situation in which the contraband was in "open, obvious view."⁵⁵

Courts have taken different approaches to the application of the plain view doctrine in the context of searches of digital evidence. For example, in *Carey*, the government insisted that its search for child pornography, although not authorized by the warrant, was nevertheless appropriate under the plain view doctrine. Although the U.S. Court of Appeals for the Tenth Circuit ultimately declined to answer the specif-

ic question of what constitutes plain view in the context of computer files, it held that, because the images were in closed files, they were not in plain view.⁵⁶

In sharp contrast, the court in *United States v. Gray*⁵⁷ held that the agent's authority to search for hacker materials and NLM documents entitled him to examine each and every file on the computer.⁵⁸ In *United States v. Wong*, the Ninth Circuit held that the officer could properly search only the types of files likely to contain evidence relating to the murder investigation at issue.⁵⁹ The outcome in *Gray* and *Wong* was effectively the same: because the officers were lawfully able to search the files that were found to contain evidence of another crime, the documents were lawfully seized under the plain view doctrine.⁶⁰

A. The Ninth Circuit's Comprehensive Drug Testing Opinion

In a potentially groundbreaking *en banc* opinion in 2009, the U.S. Court of Appeals for the Ninth Circuit effectively rejected the use of the plain view doctrine altogether within the computer search context and placed additional restrictions on the government's conduct in this area.⁶¹ The *CDT* case was "about the procedures and safeguards that federal courts must observe in issuing and administering search warrants and subpoenas for electronically stored information."⁶²

As a threshold matter, the *CDT* court "accept[ed] the reality that ... over-seizing is an inherent part of the electronic search process."⁶³ At the same time, the court recognized that the "pressing need of law enforcement for broad authorization to examine electronic records ... creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant."⁶⁴ In an attempt to "strike a fair balance between the legitimate needs of law enforcement and the right of individuals and enterprises to the privacy that is at the heart of the Fourth Amendment,"⁶⁵ the court established the procedures below to be employed in connection with applications for warrants to search electronic data.

❖ "Magistrates should insist that the government waive reliance upon the plain view doctrine in digital evidence cases"⁶⁶ and also forswear reliance on "any similar doctrine that would allow it to retain data to which

it has gained access only because it was required to segregate seizable and non-seizable data."⁶⁷

❖ "Segregation and redaction must be either done by specialized personnel or an independent third party. ... If the segregation is to be done by government computer personnel, it must agree in the warrant application that the computer personnel will not disclose to the investigators any information other than that which is the target of the warrant."⁶⁸

❖ "Warrants and subpoenas must disclose the actual risks of destruction of information [as opposed to theoretical risks] as well as prior efforts to seize that information in other judicial fora."⁶⁹

❖ "The government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents."⁷⁰

❖ "The government must destroy or, if the recipient may lawfully possess it, return non-responsive data, keeping the issuing magistrate informed

about when it has done so and what it has kept."⁷¹

The court concluded that while it hoped that these procedures would provide a "useful tool for the future," it must ultimately rely on "the good sense and vigilance of our magistrate judges [to] preserv[e] the constitutional freedoms of our citizens while assisting the government in its legitimate efforts to prosecute criminal activity."⁷²

The widespread impact of *CDT* is made apparent by the significant reaction it has provoked. In November 2009, the United States petitioned the Ninth Circuit to conduct a full *en banc* review of its decision (i.e., a review by all of the circuit's active judges as opposed to the 11 ordinarily selected for *en banc* review). In its brief in support of the petition, the government recognized that the Ninth Circuit has never granted a full *en banc* review, nor has the government ever petitioned the court to do so. Nevertheless, the government argued that "the broad issues unnecessarily addressed in the *en banc* panel's opinion are of surpassing importance and compel that extraordinary action" in light of the fact that, according to the govern-

INDEPENDENT DNA CONSULTING

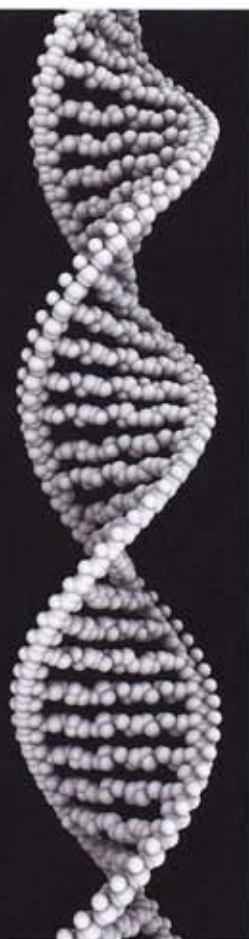
www.independentdnaconsulting.com

- Murder
- Sexual assault
- Burglary
- All DNA evidence

Rush review available

Angela Ross
(225)936-9377
info@independentdnaconsulting.com

Military defense experience



ment, the new rules are "having a sweeping and detrimental effect on law enforcement efforts."⁷³ The Ninth Circuit is still considering whether to grant a full *en banc* review. Regardless of the outcome of the case, it is apparent that the CDT opinion has raised important and potentially groundbreaking issues regarding the application of the Fourth Amendment to computer searches.

B. Competing Views

Despite the Ninth Circuit's decisive opinion in CDT, two other federal appellate courts and a district court in the Ninth Circuit have disagreed with and/or distinguished the Ninth Circuit's CDT analysis. These cases indicate that other courts may be reluctant to adopt special rules for computer searches, despite the inherent dangers that computer searches present.

In *United States v. Mann*,⁷⁴ the Seventh Circuit explicitly rejected the Ninth Circuit's CDT approach and upheld a computer search that revealed evidence outside of the scope of the warrant at issue.⁷⁵ While executing a warrant to search the defendant's computer and other electronic media for evidence of voyeurism, police officers seized a desktop computer, a laptop, and an external hard drive. While searching the data, the officer found numerous files relating to evidence of both voyeurism and child pornography. Based on this evidence, the defendant was charged with voyeurism and child pornography.⁷⁶

After the district court upheld the search, the defendant argued on appeal that the officers exceeded the scope of the warrant and, citing CDT, contended that the plain view exception did not apply. The Seventh Circuit rejected both arguments. In determining that the officer acted within the scope of the warrant, the court reasoned that because "computer files may be manipulated to hide their true contents," images of women in locker rooms could have been virtually anywhere on the defendant's computer.⁷⁷ Thus, the court held, the police did not exceed the scope of the warrant in searching the entire contents of the defendant's computer.

Despite the defendant's reliance on *Carey*, the *Mann* court distinguished *Carey* as factually distinct from the case at bar.⁷⁸ First, the court noted that the police in *Carey* were searching for documentary evidence (versus image files), whereas in the present case the police were searching for images of women, which the officer "could not search thoroughly for without stumbling upon [the

defendant's] extensive collection of child pornography."⁷⁹ The court also noted that the officer in *Carey* deliberately departed from his search for evidence of drug trafficking in order to search for child pornography, whereas in the instant case the officer found the child pornography while he was searching for evidence of voyeurism.⁸⁰

In discussing the plain view exception, the *Mann* court explicitly rejected the Ninth Circuit's CDT approach, stating that it was "inclined to find more common ground with the [CDT court's] dissent's position that jettisoning the plain view doctrine entirely in digital evidence cases is an 'efficient but overbroad approach.'"⁸¹ Rather than prohibiting the plain view exception from being invoked in computer searches, the court stated its preference for allowing the "contours of the plain view doctrine" to be developed gradually through "fact-based adjudication."⁸² As an alternative to adopting the CDT guidelines, the court "simply counsel[ed] officers ... to exercise caution to ensure that warrants describe with particularity the things to be seized and that searches are narrowly tailored to uncover only those things described."⁸³

In *United States v. Williams*,⁸⁴ issued the day after the *Mann* decision, the Fourth Circuit also disagreed with the reasoning applied in CDT and refused to apply a special standard to computer searches. In that case, the defendant was under investigation for sending threatening and sexually explicit e-mails that described the sender's desire to molest young boys.⁸⁵ Police applied for and received a warrant to search defendant's computers and electronic media for evidence of the offenses of computer harassment, threats of death or bodily harm, and threats of harm to persons on school property.⁸⁶ During the course of the search, police discovered numerous images of child pornography on both the computer hard drive and a DVD labeled "Virus Shield, Quarantined Files, Destroy."⁸⁷ The defendant argued that these images were beyond the scope of the warrant because they did not relate to any of the offenses specified in the warrant.

On appeal, the Fourth Circuit agreed with the district court's reasoning that the pornographic images were "sufficiently relevant to the crimes designated in the warrant to justify their seizure under the warrant."⁸⁸ The court also held, on alternative grounds, that the images fell within the plain view

exception. In a thorough analysis of this issue, the court concluded that the searching officer's actions met all of the elements of the plain view exception. First, it reasoned that police, when searching the contents of a computer, cannot be limited to viewing only the file names or extensions of particular documents, because "the designation or labeling of files on a computer can easily be manipulated to hide their substance."⁸⁹ Second, because police must open the files in order to view their contents, the court reasoned, they are "lawfully present" in the place from which the incriminating material may be viewed and are legally authorized to open all of the files.⁹⁰ Finally, it becomes "immediately apparent" to officers who come upon images of child pornography while conducting an authorized search that the material is incriminating.⁹¹

The *Williams* court noted that just as there is an inherent danger in searching paper files in which the contents are not readily ascertainable, the same danger exists in searches of computer files.⁹² However, the court concluded that "[w]hile that danger certainly counsels care and respect for privacy when executing a warrant, it does not prevent officers from lawfully searching the documents, nor should it undermine their authority to search a computer's files."⁹³ Finally, the court stated that it saw no reason to depart from the principles it had applied in the context of non-electronic searches.⁹⁴ Notably, the court never mentioned the CDT case in its analysis.

Finally, a recent decision in the U.S. District Court for the District of Hawaii raised questions as to whether other courts — even those within the Ninth Circuit — will adhere strictly to CDT's "principles" for electronic searches. In *United States v. King*,⁹⁵ the defendant moved to suppress computer-related evidence, arguing that the search was illegal because the magistrate judge did not comply with CDT's procedures in issuing the warrant. The court rejected that argument, distinguishing CDT on the ground that CDT involved "deliberate overreaching by the government in an effort to seize data for which it lacked probable cause"⁹⁶ while the case at hand involved evidence the police uncovered during a search that was within the scope of the warrant and supported by probable cause.⁹⁷ Rejecting a prophylactic application of CDT, the court noted that "[t]he CDT opinion itself does not claim to base its 'procedures' on the Fourth Amendment," and concluded that mere non-compliance with CDT's

"procedures" was, therefore not enough to render an otherwise valid computer search unlawful.⁹⁸ In other words, the court interpreted *CDT* to apply only to electronic searches that reveal incriminating information outside of the scope of the warrant, rather than all electronic searches that fail to conform to *CDT*'s principles. It remains to be seen whether the Ninth Circuit will affirm this interpretation of *CDT*.

C. Challenging the Government's Use of the Plain View Doctrine in the Context Of Computer Searches

Despite the differing views among courts regarding this issue, the *CDT* opinion may lead to a sea change — particularly in the Ninth Circuit — in the way that government agents and courts deal with these issues. Regardless of its long-term impact, *CDT* is certainly instructive for future challenges to the plain view doctrine's application within this context, which challenges may be based on some or all of the points outlined below.

1. Use of the plain view doctrine within the computer context undermines its original rationale and justification.

As noted, the plain view doctrine originated in physical contexts where evidence is typically tangible, discrete, and easily separable. In those circumstances, allowing the seizure of evidence under the plain view doctrine was justified because it spares the police "the inconvenience and the risk — to themselves or to preservation of the evidence — of going to obtain a warrant."⁹⁹ However, for at least two reasons, those justifications are not available in the context of a search of electronic data in a controlled environment. First, there is no actual risk of harm to police officers within a controlled, off-site environment. Second, in that scenario, law enforcement has already seized and most likely preserved the data by making a bitstream copy (i.e., a "mirror image") of the storage media. Consequently, the practical justifications underpinning the plain view exception vanish when the search relates to electronic data that has already been seized.

2. The plain view doctrine applied to computer searches raises a significant risk of pretextual dragnet searches.

In the traditional context, the U.S. Supreme Court rejected the notion

that the plain view doctrine would lead to widespread pretextual and dragnet searches, because the Fourth Amendment's particularity requirement forces the police to describe with particularity the place to be searched and the things to be seized.¹⁰⁰ In that traditional scenario, the officer is limited to searching only those places that are large enough to contain the specific physical items particularly described. This limit does not apply within the digital evidence context, where the physical size of a particular file is an amorphous concept. As a result, a computer search often reveals — arguably in "plain view" — a large volume of evidence that has nothing to do with the substance of the warrant.¹⁰¹

In short, in the digital context, the Fourth Amendment's particularity requirement does nothing to prevent an officer from obtaining a warrant for a low-level crime as a pretext for conducting a general, exploratory search for evidence of any crime. For that reason, the plain view doctrine should be confined to the physical context, where the limits the Supreme Court has contemplated actually exist. Otherwise, there is "a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant."¹⁰²

3. Applying the plain view doctrine to the computer context is unworkable.

a. Courts employ inconsistent rules.

Courts have struggled to adapt Fourth Amendment concepts to the computer search context and have disagreed as to the proper balance between ensuring that law enforcement has the tools it needs to obtain relevant evidence while also safeguarding the privacy rights of individuals and other entities. For example, the Tenth Circuit in *Carey* advocated a special approach for computer searches, concluding that analogies to physical containers or file cabinets oversimplified and ignored the realities of "massive modern computer storage."¹⁰³ In contrast, in *Williams*, the Fourth Circuit concluded that "the sheer amount of information contained on a computer does not distinguish the authorized search of the computer from an analogous search of a file cabinet containing a large number of documents."¹⁰⁴

Even those courts that accept the computer/physical container analogy

disagree as to the particular application of that analogy. For example, some courts have determined that individual files are each the equivalent of a container,¹⁰⁵ while others consider a disk with multiple files to be the container,¹⁰⁶ and still others view the entire computer or storage device as the container.¹⁰⁷ With such inconsistency in approaches and the U.S. Supreme Court having yet to offer specific guidance, it is unclear for purposes of the plain view doctrine how to address such threshold questions as whether an officer has "lawfully arriv[ed] at the position from which the object is plainly seen."¹⁰⁸

b. Is electronic data ever in plain view?

Additionally, the very nature of computer data and the searches of such data raises the question: Is electronic data ever in plain view? The essential element of the plain view doctrine requires the evidence to be "obvious to the senses."¹⁰⁹ As previously discussed, computer data at its simplest level — magnetic charges — cannot be seen directly, nor can the strings of ones and zeros these charges create be interpreted by simply seeing or observing them. Instead, software programs translate this data into useable and readable formats. This also applies on a larger level to encrypted, deleted, or hidden files. Indeed, the DOJ Manual instructs law enforcement to justify the need for wholesale seizure and off-site review of digital data by citing the possibility of encrypted, deleted, or hidden files that require specific expertise and specialized equipment to analyze.¹¹⁰ How can evidence recoverable only with the use of such specialized equipment also be "obvious to the senses" or in plain view?¹¹¹

c. Is everything in a computer search in plain view?

Law enforcement frequently requests, and courts routinely authorize, wholesale seizure of electronic data based on the argument that the relevant data may be concealed, encrypted, mislabeled, or even booby-trapped. Importantly, the government decides how much data to seize. And once seized, law enforcement often gives the same reasons to justify its examination of the contents of every file. As a result, officers may often be lawfully in a position where they can view everything on the computer that is being searched.¹¹² Indeed, both the *Mann* and *Williams* courts explicitly acknowledged that because incriminating data could have

been hidden anywhere on the defendants' computers, the law enforcement officers in question were legally entitled to search the entire contents of the computers.¹¹³ The *Mann* court even cited with approval the searching officer's testimony that "[r]egardless of what I found, I would search in all the files if I felt it necessary, if I felt that it contained information that was pertinent to my case or even exculpatory."¹¹⁴ In other words, the court took no issue with the officer's admitted intention to conduct a general search of the defendant's computer, despite the limitations set forth in the warrant.

However, the U.S. Supreme Court, in applying the plain view exception, has made clear that the exception may not be used to transform a valid search into a prohibited, general search.¹¹⁵ The Court has warned that although any evidence seized by police will be in plain view at the moment of the seizure, courts must "identify the circumstances in which plain view has legal significance rather than being simply the normal concomitant of any search, legal or illegal."¹¹⁶ Furthermore, the Court has instructed that "the plain view doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges."¹¹⁷ Because law enforcement officers often — justifiably or not — search the entire contents of a computer in executing a warrant, there is ample opportunity for officers to conduct the type of boundless searches so despised and feared by the Framers.

IV. Conclusion

The central role that computers play in our lives means that — at least with respect to actual wrongdoers — those computers will often contain evidence essential to criminal investigations. But those computers will also contain myriad other private, sensitive information that has nothing to do with the investigation at issue.

The seizure and search of electronic data presents unique challenges and illustrates the tension between the legitimate law enforcement need to search for and seize evidence, on the one hand, and the Fourth Amendment privacy interests of individuals and other entities, on the other. One of the greatest dangers within the computer context is coupling the already intrusive, invasive power of computer searches with the plain view exception to the Fourth

Amendment's warrant requirement. While courts struggle with developing appropriate safeguards in this area, it is important for counsel to understand these challenges and to develop strategies to protect against the "wide-ranging exploratory searches the Framers intended to prohibit."¹¹⁸

Notes

1. *United States v. Gray*, 78 F. Supp. 2d 524 (E.D. Va. 1999).
2. *United States v. Comprehensive Drug Testing, Inc.*, 513 F.3d 1085, 1116 (9th Cir. 2008), *rev'd en banc*, 579 F.3d 989 (9th Cir. 2009).
3. *Id.* at 1092–93.
4. *Id.* at 1116.
5. See Wayne Jekot, *Computer Forensics, Search Strategies, and the Particularity Requirement*, 7 U. PITT. J. TECH. L. & POL'Y 2, 9–11 (2007).
6. See, e.g., *United States v. Hill*, 459 F.3d 966, 975 (9th Cir. 2006).
7. *Id.* at 978.
8. NELSON LASSEN, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 31 (1937).
9. *Id.*
10. *Id.* at 53.
11. *Id.* at 54.
12. *Id.* at 59 (quoting *Works of John Adams*, X, 276).
13. The Virginia Declaration of Rights was the first American precedent for the Fourth Amendment, stating: "General warrants whereby an officer or messenger may be commanded to search person or persons not named, or whose offense is not particularly described and supported by evidences, are grievous and oppressive and ought not to be granted." *Id.* at 79 (quoting Benjamin P. Poore, *Federal and State Constitutions*, (Washington, 1877), II, 1909).
14. U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the person or things to be seized.").
15. *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).
16. See Samantha Trepel, *Digital Searches, General Warrants, and the Case for the Courts*, 10 YALE J. L. & TECH. 120, 128 (2007).
17. *Id.*
18. G. Robert McLain, Jr., *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).
19. Ray Ming Chang, *Why the Plain View*

Doctrine Should Not Apply to Digital Evidence, SUFFOLK J. TRIAL & APP. ADVOC. 31, 36 (2007).

20. McLain, *supra* note 18 at 1093–96.
21. *Id.*
22. COMPUTER CRIME & INTELLECTUAL PROP. SECTION, CRIMINAL DIV., U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 62 (2009) [hereinafter DOJ MANUAL] available at <http://www.cybercrime.gov/ssmanual/index.html>.
23. Law enforcement has frequently performed this type of search. See, e.g., *United States v. Comprehensive Drug Testing*, 513 F.3d 1085, 1135 (Thomas, J., dissenting), *rev'd en banc*, 579 F.3d 989 (9th Cir. 2009) (after seizing an entire directory pursuant to an MLB steroid investigation, agent simply "perused all of the material" within the directory, opening individual files within the file directory); *United States v. Walser*, 275 F.3d 981, 984 (10th Cir. 2001) (while in the suspect's home, the officer sat down at the computer and began opening the files within the Program Files folder, eventually opening an .AVI file containing child pornography); *United States v. Gray*, 78 F. Supp. 2d 524, 526–27 (E.D. Va. 1999) (the special agent opened directories and sub-directories within the hard drive and methodically opened files within each, ultimately finding child pornography).
24. McLain, *supra* note 18 at 1092. A deleted file is not to be confused with files in the "Recycling Bin" or "Trash Can," which could be accessed in a file-by-file search. A deleted file may be recoverable if the clusters have not been reassigned by the computer to store other data.
25. *Id.* at 1093.
26. *Id.*; see also Jekot, *supra* note 5 at 6 (noting that approximately 500 files are altered during the start-up process of a Windows operating system).
27. McLain, *supra* note 18 at 1095.
28. *Id.*; see also Jekot, *supra* note 5 at 11.
29. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 545–46 (2005).
30. DOJ MANUAL, *supra* note 22 at 86; Kerr, *supra* note 29 at 547. The DOJ separates computer searches into two stages — "imaging" and "examination." Professor Kerr refers to these stages as "data acquisition" and "data reduction."
31. Kerr, *supra* note 29 at 541.
32. In fact, the DOJ Manual encourages officers to explain in their warrant applications that "searching for information stored in computers" requires a seizure of the electronic storage device and a search by a "qualified computer expert in a laboratory or other controlled environment." DOJ MANUAL, *supra* note 22 at 245.

33. *United States v. Hill*, 459 F.3d 966, 975 (9th Cir. 2006).

34. The Ninth Circuit requires the affiant to explain why a seizure and off-site examination are necessary. *See, e.g., Hill*, 459 F.3d at 974-75.

35. *See* DOJ MANUAL, *supra* note 22 at 76-77; *see also United States v. Comprehensive Drug Testing*, 579 F.3d 989, 995 (9th Cir. 2009) (hereinafter CDT).

36. *See, e.g., CDT*, 579 F.3d at 995 (recognizing that the government had sought authority to seize far more data than it had probable cause to seize); *In re 3817 W. West End*, 321 F. Supp. 2d 953, 958 (N.D. Ill. 2004) (recognizing a substantial likelihood that computer contains documents the government has no probable cause to seize).

37. *In re 3817 W. West End*, 321 F. Supp. 2d at 958.

38. *United States v. Tamura*, 694 F.2d 591, 595 (9th Cir. 1982) (quotation omitted).

39. Other courts have rejected special protections for electronic data, such as the imposition of search protocols designed to ferret out responsive documents without exposing agents to other, irrelevant materials. *See, e.g., United States v. Hill*, 322 F. Supp. 2d 1081 (C.D. Cal. 2004) (rejecting the argument that absence of search protocol rendered the warrant overbroad). *But see CDT*, 579 F.3d at 999 (requiring that government design search protocol to "uncover only the information for which it has probable cause"); *In re 3817 W. West End*, 321 F. Supp. 2d at 955 (refusing issuance of warrant until the government provided a search protocol).

40. *Tamura*, 694 F.2d at 595.

41. *Id.* at 596.

42. *Id.*

43. *United States v. Adjani*, 452 F.3d 1140, 1149 n.7 (9th Cir. 2006).

44. Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 108 (1994).

45. 172 F.3d 1268, 1270 (10th Cir. 1999).

46. *Id.*

47. *Id.* at 1272.

48. *Coolidge v. New Hampshire*, 403 U.S. 443, 466 (1971) (plurality opinion).

49. *See, e.g., United States v. Wong*, 334 F.3d 831 (9th Cir. 2003) (admitting evidence of child pornography found while searching for evidence related to the murder of defendant's girlfriend).

50. *See, e.g., United States v. Walser*, 275 F.3d 981 (10th Cir. 2001) (during a search for evidence of drug dealing, officer discovered child pornography and successfully obtained warrant to search for additional images).

51. *See, e.g., CDT*, 579 F.3d 989 (9th Cir. 2009) (ultimately unsuccessful attempt by the government to keep evidence found in computer search relating to third parties'

steroid testing results).

52. Numerous courts and scholars have questioned the application of the plain view doctrine in this context. *See, e.g., Kerr, supra* note 29 at 583 (concluding that "abolishing the plain view exception [with respect to digital information] may best balance the competing needs of privacy and law enforcement"); Chang, *supra* note 19 at 66 (arguing that although drastic, eliminating the plain view exception in computer contexts would best protect against general searches); *see also United States v. Comprehensive Drug Testing*, 513 F.3d 1085, 1144 (9th Cir. 2008) (Thomas, J., dissenting) (stating "it is also clear why the plain view doctrine would be inappropriate to apply in the computer context"), *rev'd en banc*, 579 F.3d 989 (9th Cir. 2009); CDT, 579 F.3d 989, 1011 n.4 (9th Cir. 2009) (Callahan, J., concurring in part, dissenting in part) (acknowledging concern about the "broad application of the plain view doctrine to the search of computer data in this case").

53. *Arizona v. Hicks*, 480 U.S. 321, 326 (1987).

54. *Minnesota v. Dickerson*, 508 U.S. 366, 375 (1993).

55. *Id.*

56. *United States v. Carey*, 172 F.3d 1268, 1273 (10th Cir. 1999).

57. 78 F. Supp. 2d 524 (E.D. Va. 1999).

58. *Id.* at 528.

59. 334 F.3d 831, 838 (9th Cir. 2003) (holding that, because the agent was searching graphic files, which was allowable under the warrant, the child pornography images were in plain view).

60. *Gray*, 78 F. Supp. 2d at 528-29; *Wong*, 334 F.3d at 838.

61. CDT, 579 F.3d at 1006.

62. *Id.* at 993.

63. *Id.* at 1006.

64. *Id.* at 1004.

65. *Id.* at 1006.

66. *Id.*

67. *Id.* at 998.

68. *Id.* at 1006.

69. *Id.*

70. *Id.*

71. *Id.*

72. *Id.* at 1007.

73. Petitioner's Brief in Support of Rehearing En Banc by the Full Court at 1, CDT, Nos. 05-10067, 05-15006, 05-55354 (Nov. 23, 2009).

74. 592 F.3d 779 (7th Cir. 2010).

75. *Id.* at 785.

76. *Id.* at 780.

77. *Id.* at 782-83.

78. *Id.* at 783.

79. *Id.*

80. *Id.* at 784.

81. *Mann*, 592 F.3d at 785 (7th Cir. 2010) (quoting CDT, 579 F.3d at 1013 (Callahan, J.,

About the Authors

David Angeli, Co-Chair of NACDL's White



Collar Crime Committee, has tried a number of complex, high-profile cases around the country. He is a frequent speaker at local and national CLEs, and serves as an Adjunct Professor of Law at the Lewis & Clark Law School, where he teaches a federal white collar crime seminar.

David Angeli

Angeli Law Group LLC
1000 S.W. Broadway, Ste. 1500
Portland, OR 97205
503-222-1552
Fax 503-227-0880
E-MAIL david@angelilaw.com

Christina Schuck will graduate in May



2011 from Lewis & Clark Law School. She has served as a law clerk for David Angeli and the U.S. Attorney's Office for the District of Oregon, and as an extern for U.S. District Court Judge Michael Mosman.

Christina Schuck

Lewis & Clark Law School
10015 S.W. Terwilliger Blvd.
Portland, OR 97219
E-MAIL cmschuck@lclark.edu

Avalyn Taylor is a 2009 cum laude



graduate of Lewis & Clark Law School and an attorney at the Angeli Law Group LLC, where she focuses on environmental criminal defense. Prior to attending law school, she spent six years working as a lobbyist and congressional aide specializing in environmental policy.

Avalyn Taylor

Angeli Law Group LLC
1000 S.W. Broadway, Ste. 1500
Portland, OR 97205
503-222-1552
Fax 503-227-0880
E-MAIL avalyn@angelilaw.com