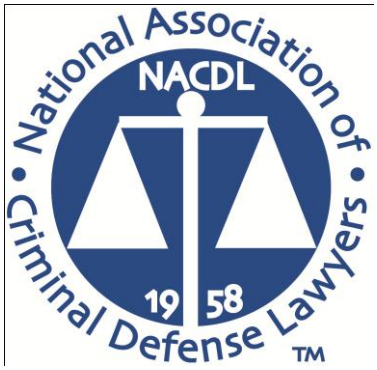

WHAT'S OLD IS NEW AGAIN: RETAINING FOURTH AMENDMENT PROTECTIONS IN WARRANTED DIGITAL SEARCHES

(PRE-SEARCH INSTRUCTIONS AND POST-SEARCH REASONABLENESS)

A Report by NACDL's
Fourth Amendment Advocacy Committee
Reporter: Steven R. Morrison

May 18, 2014

FOURTH AMENDMENT ADVOCACY COMMITTEE

Mr. Gerald H. Goldstein
Co-Chair
San Antonio, Texas

Mr. E. G. Morris
Co-Chair
Austin, Texas

Mr. Samuel A. Guiberson
Vice Chair
Iowa City, Iowa

Mr. Steven R. Morrison
Vice Chair
Grand Forks, North Dakota

Mr. Alexander Bunin
Member
Houston, Texas

Mr. Aric M. Cramer Sr.
Member
Saint George, Utah

Mr. Robert C. Gottlieb
Member
New York, New York

Mr. John Wesley Hall
Member
Little Rock, Arkansas

Ms. Dayna L. Jones
Member
Del Rio, Texas

Mr. John G. Koufos
Member
Long Branch, New Jersey

Mr. Charles W. Lammers
Member
Jacksonville, Florida

Ms. Cynthia Eva Hujar Orr
Member
San Antonio, Texas

Mr. Kenneth W. Ravenell
Member
Baltimore, Maryland

Mr. Matthew Sullivan
Member
San Francisco, California

Ms. Mason C. Clutter
National Security and Privacy Counsel
National Association of Criminal Defense Lawyers
Washington, D.C.

WHAT'S OLD IS NEW AGAIN: RETAINING FOURTH AMENDMENT PROTECTIONS IN WARRANTED DIGITAL SEARCHES (PRE-SEARCH INSTRUCTIONS AND POST-SEARCH REASONABLENESS)*

Introduction

New technologies have challenged the jurisprudence of Fourth Amendment searches and seizures. Despite the disruptive and transformational changes that digital technologies have brought to our society, the constitutional prerequisites for searches and seizures of digital evidence should be no different than searching a physical place. Neither the technological sophistication nor the diminutive physical dimensions of a device to be searched are dispositive of the privacy interests in the information stored on the device.

The fact that computers, external file storage and cloud servers are employed does not require one to alter the high threshold that must be met to justify government intrusion. Each new technology that affords a different type of private place to preserve private communications does not require a different standard for the search and seizure of its contents than is constitutionally required for the search of a file cabinet or the search of a home. What *is* different is the amount of private information that can be improperly searched and the substantially greater intrusion upon privacy and Fourth Amendment interests that may result.

One must look to the Fourth Amendment to define the limits of such searches and then ask whether the existing policies, procedures and guidelines applied to the technologies of the day appropriately mirror our fundamental constitutional values. Currently, they do not. The starting point cannot be that everything is fair game.

Today, courts are considering searches and seizures of digital evidence and what parameters, if any, should be placed on law enforcement prior to executing warranted searches of such evidence under the Fourth Amendment. Also, courts are addressing law enforcement's use of technology to gather information. For example, in *Kyllo v. United States*,[1] the Supreme Court considered the use of a thermal imager to detect activity in a private home and restricted officers' use of sense-enhancing technology. Most recently, *United States v. Jones*[2] considered the use of a GPS device to track a suspect for twenty-eight days. Although the Court's decision rested on its view that the government had committed common law trespass in putting the tracking device under the fender of the vehicle, a majority of the Court was ready to hold that tracking of the suspect, while in plain view on public streets, constituted a search.[3]

Underlying many of these cases is *Katz v. United States*,[4] which considered the warrantless use of an electronic listening device that could detect sound through walls and shifted the constitutional analysis away from a concern with "constitutionally protected areas" and toward an attention to individuals' expectations of privacy. While the private property theory of the Fourth Amendment that informed the concept of "constitutionally protected areas" was recently reinvigorated, the reasonable expectation of privacy test remains in force and applies to cases involving the intersection of technology and personal privacy.

Unfortunately, these cases are improperly analogized to law enforcement searches of digital evidence. These cases actually address the real-time collection of data—whether location tracking, a conversation between two or more participants, or the heat image of a home. Digital searches of evidence, however, are actually better addressed by case law discussing law enforcement searches of papers and effects under the Fourth Amendment. Documents on a hard drive are really digital papers, much like the papers stored in a desk drawer that the Founders considered while drafting the Constitution. The reasonable expectation of privacy test, therefore,

is an inappropriate starting point for computer searches.[5] Because the search of a digital device for evidence of a crime constitutes the search of an effect for private papers, the Fourth Amendment requires that law enforcement, in the absence of any exception, obtain a warrant to seize and search that device and its contents. This report addresses what such a warrant application, and the warrant itself, should include in light of today's digital realities.

The storage of massive amounts of personal information on digital devices such as computers, cell phones, external hard drives, and flash drives — and the way that this information is stored — presents a unique technological advent[6] that challenges current Fourth Amendment law. Privacy advocates are proposing new rules to protect private digital information, while law enforcement agencies are generally relying on traditional search warrant law to sustain extensive and sometimes overly-intrusive searches of digital devices. Courts are attempting to balance the competing needs for both citizens' privacy and effective law enforcement.

Many courts have already considered some fundamental questions: first, should digital devices be treated as mere containers,[7] or should they be treated as unique because of the amount of data they contain[8] or their small physical scale or virtual character compared to traditional containers? In other words, a limited amount of information may be kept in a physical container like a cigarette case or a briefcase, whereas an exponentially greater amount of information may be stored on a laptop or a smartphone. Should this distinction be dispositive of the Fourth Amendment rights afforded to physical and digital storage? Second, does the nature of digital data — voluminous, potentially difficult to find, easy to conceal,[9] difficult to control and destroy[10] — call for greater deference to agents who execute search warrants[11]or for greater judicial oversight?[12] In any event, magistrates in the last decade have increasingly included pre-

search instructions in digital device warrants,[13] with varying responses from appellate courts about whether such instructions ensure citizens' privacy or excessively hinder law enforcement.

From the National Association of Criminal Defense Lawyers' ("NACDL") perspective, the default must be the protection of privacy and Fourth Amendment rights. This report addresses warranted searches of digital devices, specifically what the underlying applications for a warrant should include and what restrictions magistrates should place on the search and seizure of private data *before* the warrant is executed.[14] First, it sets forth a discussion of digital data storage, search, and seizure and the specific constitutional issues arising from them. Second, it discusses pre-search instructions: what they are, how courts have responded to them, and what their merits and drawbacks are. Finally, the report makes recommendations for legislative and judicial reform that account for the reality of digital searches. These recommendations draw from the use of both post-search reasonableness analysis and pre-search instructions.

I. Digital Realities

Often, realities inherent in digital searches give rise to the conflict between law enforcement efforts to uncover evidence of crime and citizens' privacy. The primary reality is that at first glance, the content of digital data is not readily apparent. For instance, documents not relevant to a criminal investigation may be co-mingled with evidence of a crime, or files and file extensions may be named to conceal criminal activity or protect personal privacy.[15] Files can also be moved, copied, and stored on more than one device. And, files may exist on digital devices without the user's knowledge, either because she "deleted" files (which really just places them in unused space on the hard drive) or because her computer automatically downloaded data and placed it in the hard drive's memory.[16] Often, agents argue that prior to opening a file, they will not be able to tell whether a particular file contains evidence of a crime.[17]

These possibilities have led to the inevitable overseizure and oversearching of digital data.[18] They have also led to arguments that officers must be permitted to open even innocuous-looking files to confirm their true contents.[19] Due to the amount of data to be sifted and the time and technical expertise required[20] to do so, off-site searches of mirrored digital devices have become the norm.[21]

In light of these representations, courts have reached two different conclusions. Some courts focus on the overseizure and oversearch realities and propose the use of pre-search instructions to appropriately structure and limit the scope of warranted searches.[22] Other courts focus on non-discernibility representations and reject such instructions in favor of the traditional post-search reasonableness analysis.[23] The goal to facilitate complete, good-faith warranted searches while protecting citizens' privacy seems impossible, as the solutions appear to be either overly-restrictive limitations on warrants on the front end or a continued reliance on the outdated reasonableness analysis on the back end. Some argue that the former entails constitutionally unauthorized and unwise requirements, which are unenforceable,[24] while others argue that the latter violate citizens' Fourth Amendment rights by enabling the execution of general warrants.[25]

II. Post-Search Reasonableness and Pre-Search Instructions

Currently, courts review warrants and their execution for reasonableness after they have been returned, with an inventory of any property seized, to the magistrate named on the warrant.[26] Pre-search instructions, in turn, consist of magistrates' requirements for the execution of warrants that go beyond traditional limits involving place-to-be-searched and things-to-be-seized particularity. These instructions are designed to address digital realities by prescribing methods by which officers must execute warrants and handle seized evidence.

The Ninth Circuit's opinion in *United States v. Comprehensive Drug Testing* (*CDT*) has been given a lot of attention[27] because of Chief Judge Kozinski's concurring opinion, in which

he advocated for magistrates' use of five pre-search instructions. In *CDT*, the court considered the execution of a warrant to search the digital records of Comprehensive Drug Testing, a facility that administered tests on hundreds of major league baseball players for steroid use.[28] Although the warrant was based on probable cause to believe that only ten players had broken the law,[29] "the government seized and promptly reviewed the drug testing records for hundreds of players in Major League Baseball (and a great many other people)."[30] Every one of the numerous judges who reviewed this search and seizure cited the government's bad faith conduct, including "manipulation and misrepresentation,"[31] failure to comply with precedential procedures regarding third party searches,[32] and "misconduct and unlawful seizure of evidence."[33]

To justify its broad seizure,[34] the government noted in its search warrant application the "generic hazards of retrieving data that are stored electronically."[35] The magistrate judge therefore permitted the government to seize virtually all computer equipment found along with any data storage devices and related materials.[36] The magistrate did, however, require that the government comply with Ninth Circuit precedent set forth in *United States v. Tamura*.[37] *Tamura* provided that where large amounts of innocuous material and possibly incriminating evidence were intermingled, a third party — not the person or entity in possession of the seized evidence and not the agents who performed the search or members of the investigatory or prosecution team — could be required to perform an initial review and segregation of data, and to determine whether this review and segregation could be performed on the site of the search and seizure.[38] The government in *CDT* ignored this requirement as well as the requirement that trained computer personnel perform the initial review and segregation, even though it had agreed to abide by these strictures.[39]

Having seized evidence that implicated players not included in the original search warrant in steroid usage, the government relied on the plain view doctrine, arguing that it could

not be sure what was in each nook and cranny of the seized computers without searching them.[40] The plain view doctrine provides, in short, that law enforcement agents may seize anything they observe if the object's incriminating character is immediately apparent and if the agents have arrived at their vantage point lawfully. In *CDT*, the government did not claim that it seized this beyond-the-warrant evidence inadvertently; it admitted that "the idea behind taking [the evidence] was to take it and later on briefly peruse it to see if there was anything above and beyond that which was authorized for seizure in the initial warrant."[41] The court concluded that the "government agents obviously were counting on the search to bring constitutionally protected data into the plain view of the investigating agents."[42]

Surprising as it may seem, the government's admission that it intended to seize evidence beyond the scope of the warrant is grounded in law. In *Coolidge v. New Hampshire*, the Supreme Court first explicitly established that to rely on the plain view doctrine to seize evidence that was beyond the scope of a warrant, agents must have arrived at the evidence unintentionally.[43] In turn, where "discovery is anticipated," agents may not rely on plain view.[44]

Nearly 20 years later, in *Horton v. California*, however, the Court rejected the inadvertence requirement,[45] mandating only that agents come to evidence in plain view lawfully — that is, within the scope of the warrant — and that the incriminating character of the evidence be "immediately apparent."[46] This means that during a warranted search for evidence of credit card fraud, if agents come across a folder labeled "kiddiepornpics," agents may nevertheless perform a detailed search of the contents of that folder, even if they intend to find evidence of child pornography and not credit card fraud.[47] This is so because of the general non-discernibility of digital evidence; a file labeled "kiddiepornpics" could technically contain evidence of credit card fraud. In the digital context, the government argues, this means that once a warrant to search digital devices issues, agents may search the entirety of the devices, even if

they are attempting and expecting to find evidence of *any* crime, whether or not it is set forth in the warrant. This cannot be the case.

The per curiam *CDT* panel, Judge Bea and Chief Judge Kozinski, offered three important but contradictory responses to this result. The per curiam opinion affirmed the lower courts' post-search findings that the government's search of the digital evidence was unreasonable because it "circumvent[ed] or willfully disregard[ed] limitations in [the] search warrant"[48] and failed to follow the *Tamura* requirements, i.e., third party screening and segregation of digital information.[49] Judge Bea, concurring in part and dissenting in part, argued that the evidence in question was not in plain view; to see the evidence of players other than the original ten suspected of steroid use, agents had to take specific, unwarranted action.[50] Judge Bea's opinion, therefore, focused on a specific example of the failure to follow warrant requirements with which the per curiam opinion was concerned. Both opinions rested on existing Fourth Amendment law, which includes searches limited by warrants, the reliance on the *Tamura* precedent, and post-search reasonableness analysis.

Chief Judge Kozinski departed from precedent by providing five pre-search guidelines. These guidelines, he explained, "will significantly increase the likelihood that the searches and seizures of electronic storage that they authorize will be deemed reasonable and lawful."[51] The five guidelines are:

> 1. Magistrate judges should insist that the government waive reliance upon the plain view doctrine in digital evidence cases.
>
> 2. Segregation and redaction of electronic data must be done either by specialized personnel or an independent third party. If the segregation is to be done by government computer personnel, the government 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.
>
> 3. Warrants and subpoenas must disclose the actual risks of destruction of information as well as prior efforts to seize that information in other judicial fora.

> 4. 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.
>
> 5. 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.[52]

While pre-search instructions are controversial, some of them are necessary to ensure the particularity of places to be searched and things to be seized. As the Vermont Supreme Court observed:

> In the digital universe, particular information is not accessed through corridors and drawers, but through commands and queries. As a result, in many cases, the only feasible way to specify a particular 'region' of the computer will be by specifying how to search. We view such ex ante specification as an acceptable way to determine particularity.[53]

In general, pre-search instructions may be required where they are necessary to ensure particularity and are functional, meaning that they do not prevent agents from executing searches up to the bounds set by the search warrant.[54]

It is argued that the question is zero sum: courts must choose either post-search reasonableness or pre-search instructions. If they choose the former, agents will be able to perform searches completely, uncovering incriminating evidence while excessively invading privacy. If they choose the latter, privacy will be preserved, but law enforcement effectiveness will be decimated and agents' right to execute warrants according to their terms will be thwarted. This zero sum assumption, however, is uninformed because it is not nuanced and does not recognize that pre-search instructions and post-search reasonableness are both important to ensuring privacy and can work together. A discussion of each of Judge Kozinski's guidelines is necessary to understand the nuances.

A. Foreswearing Reliance on Plain View

Pursuant to the plain view doctrine, if agents are where they are legally permitted to be and observe something whose incriminating character is immediately apparent, they may seize the item and it will generally be admissible in court, at least from a Fourth Amendment perspective.[55] If the incriminating character of the evidence is not immediately apparent, plain view does not justify seizure or further inspection of the item.[56] Agents must have probable cause to believe the item is incriminating.[57]

In a sense, anything that agents observe is in plain view, whether the agents arrive at their vantage point legally or illegally.[58] The applicability of the plain view doctrine, therefore, depends upon agents arriving at their vantage point legally.[59] As long, however, as agents performing a warranted search do so within the place-to-be-searched and things-to-be-seized strictures of the warrant, their subjective intent is irrelevant. In other words, if an agent is executing a warrant to search for evidence of mail fraud, but thinks he may also find child pornography, as long as he is within a place he is legally permitted to be under the warrant, evidence of child pornography is fair game.[60] The permissibility of a search is instead defined "*objectively* by the terms of the warrant and the evidence sought, not by the *subjective* motivations of an officer."[61] This should be no different when agents are searching for digital data rather than physical evidence.

At the same time, plain view is an exception to the warrant requirement that should be "as limited as possible" by the "magistrate's scrutiny [that] is intended to eliminate altogether searches not based on probable cause."[62] Plain view cannot justify a search beyond the bounds of a warrant; if it did, warrants would become general.[63]

Courts have taken four approaches to the plain view doctrine in the context of digital searches. First, some courts freely apply it while rejecting most or all other pre-search instructions, relying solely on post-search reasonableness analysis.[64] Second, other courts have

apparently imposed an inadvertence requirement for the application of plain view, even though *Horton* did away with it. The exception in these jurisdictions is that agents may perform *cursory* surveys of unknown files to determine their contents. In these courts, if a warrant is granted to search for and seize evidence of crime 1, and an agent inadvertently discovers evidence of crime 2, the agent must cease the search and obtain a new warrant. She may not rely on the argument that it is impossible to know what something is until it is searched to continue her search.[65]

Third, in an opinion supportive of pre-search instructions, the Vermont Supreme Court held that magistrates may not condition the issuance of a warrant on agents abandoning their right to seize evidence found in plain view. The use of filter teams, said the court, would render abandonment of plain view unnecessary, and, in addition, courts are not permitted to "alter what legal principles will or will not apply in a particular case."[66] Fourth, Kozinski's *CDT* guidance would require agents to abandon reliance on plain view altogether.[67]

What it means to abandon or foreswear reliance on plain view is not immediately apparent, and Kozinski's *CDT* concurrence did not clarify his position. Other courts, however, have weighed in. For example, the Second Circuit, Eleventh Circuit, and a California District Court suggested that the right to seize evidence in plain view could be unavailable if agents intentionally searched for evidence not covered by the warrant.[68] This approach would permit agents to perform intensive searches that are within the particularity bounds of warrants, and to address non-discernibility by performing cursory surveys of unknown digital files. It would not, however, permit agents to go beyond the scope of the warrant or to use non-discernibility as a pretext for engaging in what would amount to general searches.

Unfortunately, this approach is difficult to execute because the agents who performed the search could, and would, testify that they did not intentionally search for evidence not covered by the warrant. Instead, the best practice for searches of digital evidence should require agents to

agree pre-search—within the four corners of the warrant—not to rely on plain view during the execution of the warrant.

This approach fits well into both pre-search instruction and post-search reasonableness models. It fits well into pre-search instruction regimes because magistrates can inform agents that they will approve of warrant executions only where agents searched for evidence mentioned in the warrant, performed cursory searches of folders and files whose contents were unknown, and did *not* perform pretextual searches. This approach also would require post-search reasonableness analysis, as magistrates will then determine the scope of the search and whether the agent intentionally went beyond what was warranted.

Even if every nook and cranny of a digital device could *theoretically* contain evidence covered by the warrant, it does not mean that every nook and cranny may *reasonably* contain such evidence. Cursory surveys under this approach would be permissible and would show whether a particular piece of digital material is evidence covered by the warrant, in which case it is seizable; innocuous evidence, and thus not seizable; or evidence of a different crime. If the last event occurs, agents would need to cease the search and obtain a new warrant for the new crime. This is consistent with the limited nature of warranted searches, and has been practiced by many law enforcement agencies and uniformly approved by courts.[69] By contrast, courts have criticized searches that have continued after agents discovered evidence of a different crime.[70]

B. Segregation and Filter Teams

Some courts have required that third parties conduct initial reviews of seized digital materials to segregate the relevant evidence from the innocent information. Referred to as "filter teams," "privilege teams," or "taint teams,"[71] these teams currently may be part of the law enforcement agency or the prosecutor's office directing the search,[72] or they may be independent

or appointed by the court.[73] It is better policy, however, that these teams not be associated with law enforcement or prosecutors' offices. A system of segregation and use of truly independent filter teams has been cited as an effective way to avoid overseizure and general searches.[74] In fact, in the civil context, mirroring digital devices — i.e., creating an identical copy of a digital device for in-depth analysis — is discouraged because it entails overseizure,[75] and the remedy is often the use of filter teams.[76]

Several state courts have reacted favorably to the use of filter teams. The Vermont Supreme Court asserted that the use of filter teams would avoid the problems associated with abandoning reliance on plain view because any evidence coming to agents' attention would already have been vetted by the filter team.[77]

NACDL has concerns that the use of a filter team could invite overbroad searches, which would lead to minimization of the invasion of privacy and Fourth Amendment interests after-the-fact. In other words, the use of a filter team should not per se invite the team members to look at every single piece of data on a hard drive. A filter team inspection is simply a continuation of a Fourth Amendment governed search and, therefore, subject to the same parameters of the warrant as a physical search, including the limits on plain view. Once the information has been collected and searched, the invasion of privacy has already occurred, regardless of who actually looked at the information.

In line with some of these concerns, the Massachusetts Supreme Judicial Court has imposed four requirements for the use of filter teams: (1) team members may not have been or be involved in any way in the investigation or prosecution at issue; (2) team members must be prohibited from disclosing to the investigation/prosecution team both search terms submitted by defendants and any information contained in e-mails; (3) the defendants must have an opportunity to review the team's work and contest any privilege determinations made by the

team; and (4) team members must agree to these terms in writing.[78] Should a filter team be used, NACDL supports these requirements.

C. Disclosure of Actual Risks

Aside from the *CDT* opinion, courts have been largely silent on whether warrant applications ought to contain a disclosure of the actual risks of concealment and/or destruction of evidence associated with a particular requested search, or whether resort to general statements about theoretical risks of all digital searches suffices. A disclosure of the *actual* risks of destruction or concealment, however, would help the magistrate issue an appropriately limited warrant. Magistrates should, therefore, inquire into the actual issues of destruction and concealment of evidence pertaining to specific suspects. These actual risks should guide the scope of the warrant—the smaller the risks, the narrower the scope of the warrant should be drawn. Agents seeking warrants, furthermore, should not be permitted to obtain broad scope warrants based on generalizations about risk. They should obtain broad scope warrants only to the extent that they are able to demonstrate actual risks.

D. Search Protocols

Agents regularly use and courts have looked favorably upon search protocols,[79] which include keyword searches,[80] use of hashing tools for looking up or comparing data,[81] use of other forensic software like EnCase,[82] searches for only certain types of files, and any other pre-search plan. Other courts have rejected their use, accepting the argument that a document's contents are unknown until it is searched, and the magistrate's pre-search inability to determine the propriety of any particular protocol.[83] So far, no court has *mandated* protocols, preferring instead a case-by-case approach to evaluating their propriety.[84] In *CDT*, Judge Kozinski argued "these and similar search tools should not be used without specific authorization in the warrant . . . ."[85]

E. Destruction or Return of Data

Once agents have mirrored, or copied, digital evidence, they often seek to hold it for months or even years. Some magistrates have mandated destruction and return requirements for data other than data for which probable cause is shown, including copies. These requirements are not very controversial because they do not negatively affect the law enforcement endeavor: agents may retain incriminating evidence and must destroy or return only evidence that is not relevant. Furthermore, in the absence of other requirements, agents retain complete control over the digital evidence and may generally determine for themselves which evidence is incriminating and which evidence must be destroyed or returned. No court has prohibited pre-search destruction/return requirements.

III. Recommendations for Reform

While NACDL recognizes that the Fourth Amendment and Federal Rule of Criminal Procedure 41 do not facially mandate pre-search restrictions on law enforcement searches for digital evidence, NACDL nonetheless believes such restrictions are essential to protecting the right to privacy and Fourth Amendment interests in the digital age. The burden is always on law enforcement to justify the particular steps they believe are necessary to discover evidence when intruding on constitutionally protected space. The technologies at issue should not trump the privacy interests at stake. The historical roots of privacy protections run deep, and the relationship to what computers can do and store should not dilute the quantity or quality of privacy protections.

Hardware and software are no different from a bound private journal on a desk simply because they are digital in nature. The government is not allowed to seize entire buildings or homes to search for evidence of credit card fraud, and similar limits must be established for

digital searches. Policies and guidelines must be put in place by magistrates, criminal courts, and legislatures to ensure that the Fourth Amendment is protected in the digital age.

While Judge Kozinski's pre-search guidelines in *CDT* caused a stir among some courts and criminal law scholars, NACDL believes they provide a solid foundation that appropriately balances citizens' Fourth Amendment rights and the need of law enforcement to conduct searches for digital evidence of crime. A practicable solution to the privacy problems inherent in digital searches must respect both of these interests and NACDL believes that its recommendations achieve this balance.

Ideally, pre-search instructions for warrants would be mandated by statute. As in the wiretapping context, some new technologies require different judicial approaches. But, post-search reasonableness analyses cannot be abandoned altogether for pre-search instructions. While not constitutionally mandated, legislatures can always provide more protections than the Constitution provides, and NACDL encourages state and federal legislatures to pass legislation implementing the recommendations outlined in this report. In the absence of legislation, magistrates and law enforcement agents should mandate and abide by NACDL's recommendations. To that end, this report makes the following nine recommendations:

1. Magistrates should be required to impose pre-search mandates when necessary to ensure particularity of places to be searched or things to be seized.

This recommendation simply provides that magistrates should use the tools set forth in Judge Kozinski's concurrence in *CDT* — and used by countless other courts and government agents — to ensure that particularity requirements are satisfied. As discussed previously, Kozinski's pre-search guidelines are:

> 1. Magistrate judges should insist that the government waive reliance upon the plain view doctrine in digital evidence cases.
>
> 2. Segregation and redaction of electronic data must be done either by specialized

> personnel or an independent third party. If the segregation is to be done by government computer personnel, the government 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.
>
> 3. Warrants and subpoenas must disclose the actual risks of destruction of information as well as prior efforts to seize that information in other judicial fora.
>
> 4. 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.
>
> 5. 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.[86]

Law enforcement agents should be prohibited from searching where they do not have probable cause to search. Particularity requirements will aide in reigning in overbroad seizures and searches of digital evidence.

Such particularity requirements include identifying whether the hardware itself is evidence of a crime, i.e., contains contraband or is contraband, or is an instrumentality of a crime, or if the hardware simply stores evidence of a crime.[87] In general, the warrant affidavit would swear to facts that establish probable cause that evidence of a crime, like computer files, may be found in a protected space or effect, like a computer, within a private space, like a home or office.[88] The application should focus on the content of relevant files rather than the digital media itself. Agents should also identify records that relate to the particular crime for which they have probable cause to search, including specific categories of or types of records to be found. This type of information can be discerned by, for example, the identity of the target of the search, the time frame of the crime being investigated, or the actual crime itself, like child pornography.[89]

The particularity requirements for a warrant to search for digital evidence should be extensive enough to clearly and unambiguously inform law enforcement as to what is included

and what is not included within the scope of the approved search. To accomplish that objective, the articulation of the specific target of the search must utilize the narrowest particulars necessary to discriminate between what is and is not to be searched.

Take, for example, a search of a personal laptop computer to obtain evidence of a physician's alleged illegal distribution of pain medications. The warrant first must specifically identify the physical address where the computer is to be found and the location on the premises where it is located. The warrant must also specify the type of computer to be searched (in this case a specific make of laptop), and then specify the type and content of digital files to be searched. Such file types and content would be limited in this example to text documents in which search queries reveal the presence of the doctor's DEA number, names and addresses of patients referenced in the prescriptions, and emails to and from those patients. Without more supporting investigative information, the image files on the computer, other emails, and personal documents not specific to the doctor's prescription authority would be excluded from the warrant to search. Such particularities carve out the scope of the warranted search from the general population of files stored on the laptop.

Search protocols should be outlined for how the government plans to conduct onsite and offsite searches of digital devices. Agents should explain how these protocols will keep them within the bounds of the warrant. Such protocols may include the use of a third-party review team, restrictions on information sharing between the review team and law enforcement investigators and prosecutors, obtaining a warrant when evidence of a separate crime is legitimately within plain view, the use of search terms, and the use of forensic software.

Reasonable and function, this mandate would not hinder law enforcement from searching in the locations and for the things to which their probable cause attaches.

2. The remedy for government agents' failure to follow pre-search mandates imposed by magistrates should be suppression of any evidence found as a result of the search.

Agents who ignore a magistrate's pre-search instructions are acting unconstitutionally, and as a general rule any evidence they seize should be suppressed. This remedy should be included in any legislative reform regarding pre-search warrant restrictions.

3. Magistrates should continue to perform traditional post-search reasonable analyses.

Although they were originally fashioned as mandates,[90] Kozinski's pre-search instructions became admonitory guidelines that magistrates should consider but need not follow.[91] They therefore set forth a flexible structure that magistrates should apply on a case-by-case basis to ensure both privacy and effective law enforcement.[92] NACDL recognizes that these recommendations will not always be one-size-fits-all in light of facts and circumstances it cannot reasonably predict. That is why it is imperative that this structure retain the post-search reasonableness inquiry, but it should also include explicit attention to *CDT*'s ex ante guidelines, as the first recommendation above provides.

In addition, agents should proactively self-impose them in warrant applications wherever possible. This is, in fact, what many magistrates and agents already do, and so this proposal is not revolutionary. The warrant's inclusion *and* compliance with specific pre-search instructions — whether imposed as mandates by magistrates or volunteered by search warrant applicants — should be weighted in favor, but not dispositive, of a reasonableness finding. Use of the *CDT* guidelines should not relieve the government of its burden of proving reasonableness.

4. Require agents to foreswear reliance on the plain view doctrine.

Foreswearing reliance on plain view would prevent agents from executing searches beyond the original warrant's particularity limits. This would mean that searches of places and searches for things beyond those covered by the warrant would be pointless because any evidence found would be subject to suppression. Agents would still be permitted to search within the places and for the information outlined in the original warrant; however, if evidence of a new crime not covered by the original warrant is discovered, agents would then need to secure a new warrant to search for evidence of the newly discovered crime.

When agents have a warrant to search for evidence of crime 1, they should be prohibited from searching within the place-to-be-searched bounds of the warrant for evidence of crime 2, which would not be covered by the warrant's things-to-be-seized provisions. Requiring inadvertence would permit agents to perform cursory surveys of files whose contents are unknown, but, once they find evidence of crime 2, would compel them to stop searching for additional evidence and obtain a new warrant.

This is a necessary restriction in light of the oft-cited argument that digital evidence is difficult to recognize without inspection. A simple line in the warrant itself that says that the agents will not rely on the plain view doctrine during the search should suffice.

5. A second warrant should be required for agents to obtain evidence of a crime not covered by the original warrant.

Agents should stop a warranted search if evidence of a crime not covered by the warrant emerges. They then must obtain a warrant to search for the new evidence of a separate crime. Already, agents often cease their search for evidence of crime 1 when they uncover evidence of crime 2 and apply for a new search warrant. They probably do so to ensure that any evidence of crime 2 they eventually uncover will not be suppressed. This practice should be required in the digital search context. In order to effectuate this recommendation, law

enforcement officers must be required to foreswear reliance on the plain view doctrine, as discussed in recommendation three.

6. "Filter Teams" must be independent from the criminal investigation and prosecution and bound by the terms of the warrant.

As discussed in Section II B, NACDL has concerns regarding the use of third-party filter teams. However, if a filter team is used, the following guidelines must be employed. The members of the filter team must be independent from any governmental agency that had been, is, or may be involved in the criminal investigation or prosecution at issue. Further, the filter team may disclose only incriminating evidence that was the subject of the warrant. It may not disclose incriminating evidence that was not covered by the warrant, nor may it disclose innocuous information. Finally, the defendant must have an opportunity to inspect the filter team's segregation of data and contest any privilege determinations made by the team.

7. Warrants should include provisions for the destruction or return of digital information as appropriate.

As provided in Judge Kozinski's guidelines:

> [W]ithin a time specified in the warrant, which should be as soon as practicable, the government should provide the issuing officer with a return disclosing precisely what it has obtained as a consequence of the search, and what it has returned to the party from whom it was seized. The return should include a sworn certificate that the government has destroyed or returned all copies of data that it's not entitled to keep. If the government believes it's entitled to retain data to which no probable cause was shown in the original warrant, it may seek a new warrant or justify the warrantless seizure by some means other than plain view.[93]

8. Agents must retain records of the particularities of the digital search, which should be shared with defendants in criminal cases.

The warrant should include pre-search mandates that require law enforcement to keep a written record of how, where and by whom the digital search was executed. In particular, the magistrate should consider including mandates that require law enforcement to make a record of the following:

- The techniques used to examine the hard drive
- The protocols and search methodology used
- How the data will be segregated and how it was segregated
- The identification of individuals who participated on the review team, if a review team was used
- Whether any copies of digital information were made and retained, and the legal basis for such
- The return inventories should include the hardware seized and the data searched
- The search terms used
- The post-seizure strategy for screening out privileged info
- The standard that was used to determine whether information is privileged
- Whether any information was recovered from deleted files
- The "process of sorting, segregating, decoding and otherwise separating data (as defined by the warrant) from all other data . . . ."[94]

9. Legislatures should pass laws to guide courts in analyzing the reasonableness of searches conducted pursuant to warrants containing pre-search requirements.

Legislation is the most favorable road toward achieving the proper balance of interests between law enforcement and individual privacy. Any legislation seeking to address this particular issue—law enforcement searches of digital evidence—should require certain static pre-search instructions and a post-search reasonableness finding. This process would incentivize privacy-protective search and seizure practices, which should include:

1. the issuance of warrants that are as particular as possible;
2. the execution of warrants that remain within the bounds of the warrant;
3. good-faith, cursory examination of digital files whose contents are unknown;
4. immediate cessation of a search if evidence of a crime for which a warrant was not issued emerges, and a requirement for law enforcement to obtain a new warrant for that new evidence;[95] and
5. suppression of evidence obtained in violation of the pre-search mandates imposed by magistrates in a warrant.

This information should be made available to defendants in the discovery phase of a criminal trial, along with the underlying warrant application, affidavits, and warrant or orders pertaining to the warrant.

Conclusion

The use of warranted searches of digital devices is an intrusive investigative tool that is amenable to reform to safeguard citizens' privacy without impeding the public safety function of law enforcement.

Solutions to rebalance the privacy-public safety relationship may entail rigid rules. The best solution to the problem of warranted digital searches is a hybrid approach that guides judicial review with applicable criteria but also permits courts to engage in a more holistic inquiry. This report recommends such a hybrid approach. The recommendations in this report should be adopted by courts now, but eventually legislation should be passed by federal and state legislatures to require statutory compliance with the pre-search instructions and post-search reasonableness analysis outlined in this report.

Post-search reasonableness should remain an important part of the evaluation of warrant executions, just as voluntariness in the interrogation setting and individualization in the sentencing context serve justice. But the inquiry should be guided by the important pre-search instructions suggested by Judge Kozinski in *CDT*. This hybrid approach would serve justice, protect citizens' privacy by limiting the scope of searches, and ensure effective law enforcement.

[*] The National Association of Criminal Defense Lawyers (NACDL) and the Fourth Amendment Advocacy Committee ("the Committee") sincerely thank Steven R. Morrison, Assistant Professor of Law, University of North Dakota School of Law and Vice Chair of the Fourth Amendment Advocacy Committee, for his extensive researching and drafting work on this white paper, and for his work in guiding Committee members to consensus on these issues. NACDL and the Committee also thank former National Security and Privacy law clerks Ashley Chin Richardson (2012) and Natalie Salvaggio (2013) for their research in anticipation of and preparation for this white paper. Also, NACDL and the Committee thank NACDL's White Collar Crime Committee for reviewing and editing this white paper. Finally, NACDL and the Committee thank National Security and Privacy Counsel Mason Clutter for her work on this white paper.

[1] *Kyllo v. United States*, 533 U.S. 27 (2001).

[2] *United States v. Jones*, 132 S.Ct. 945 (2012).

[3] Justice Sotomayor's concurring opinion agreed with four members of the court that a trespass had occurred, which constituted a search. However, she went on to observe that the "trespass" analysis is outdated and of little use in applying the spirit of the Fourth Amendment to the realities of modern life which include, advanced surveillance and tracking technology, and the average citizen's extensive exchange of information with third parties, such as cell phone providers, banking institutions, and merchants. She suggested that the Court's established Fourth Amendment jurisprudence should be re-examined in light of the increasingly sophisticated ways that the government may now track a person's movements and activities. *See Jones*, 132 S.Ct. at 957.

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

[5] *See, e.g.*, Brief for Cato Institute as Amicus Curiae Supporting Petitioner, Riley v. California, 2014 WL 2864483 (No. 13-132) (2014).

[6] *United States v. Carey*, 172 F.3d 1268, 1275 (10th Cir. 1999) (per curiam) ("[A]nalogies to closed containers or file cabinets may lead courts to 'oversimplify a complex area of Fourth Amendment doctrines and ignore the realities of massive modern computer storage." (quoting Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV.J.L. & TECH. 75, 104 (1994))); *see also United States v. Walser*, 275 F.3d 981, 986 (10th Cir. 2001) ("analogies to other physical objects . . . do not often inform the situations we now face as judges when applying search and seizure law"); *United States v. Campos*, 221 F.3d 1143, 1148 (10th Cir. 2000) ("[T]he storage capacity of computers may require law enforcement officers to take a special approach.").

[7] *See United States v. Williams*, 592 F.3d 511, 523 (4th Cir. 2010) ("[T]he 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."); *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999) ("[A] search of a computer and co-located disks is not inherently more intrusive than the physical search of an entire house for weapons or drugs."); Office of Legal Educ. Exec. Office for United States Attorneys, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, Dep't of Justice: Computer Crime and Intellectual Property Section, Criminal Division, 2-3 (2009), http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf [hereinafter *DOJ Manual*].

[8] *See United States v. Riccardi*, 405 F.3d 852, 862 (10th Cir. 2005); *Smallwood v. State*, 113 So. 3d 724, 732 (Fla. 2013) ("[A]nalogizing computers to other physical objects when applying Fourth Amendment law is not an exact fit because computers hold so much personal and sensitive information touching on many private aspects of life.").

[9] *State v. Bizewski*, No. UWYCR110144340, 2013 WL 1849282, at *13 (Conn. Super. Ct. Apr. 10, 2013).

[10] Eric Yeager, *Looking for Trouble: An Exploration of How to Regulate Digital Searches*, 66 VAND. L. REV. 685, 690 (2013).

[11] *See United States v. Flores-Lopez*, 670 F.3d 803, 805 (7th Cir. 2012); *United States v. Bonner*, No. 12CR3429 (WQH), 2013 WL 3829404, at *19 (S.D. Cal. July 23, 2013); *Bizewski*, 2013 WL 1849282 at *13.

[12] *Smallwood*, 113 So.3d at 732.

[13] Athul K. Acharya, *Semantic Searches*, 63 DUKE L.J. 393, 409 (2013).

[14] The report does not, therefore, consider searches of devices incident to arrest, consent searches, inventory searches, border searches, probation or parole searches, or accessing digital data through third parties, such as Internet service providers. These are important and complex topics, which deserve special attention that is beyond the scope of this report. The reality of cloud computing, for example, presents special complexities. *See State v. Bellar*, 217 P.3d 1094, 1110 n.10 (Or. Ct. App. 2009). For example, the search of a cell phone with the "iCam" application could allow officers conducting a search incident to an arrest outside of a home to access the arrestee's home computer webcam and survey the insides of the home. *Smallwood*, 113 So.3d at 732.

[15] *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1168 (9th Cir. 2010) [hereinafter *CDT*].

[16] *In re Search Warrant Application*, 770 F.Supp.2d 1138, 1145-46 (W.D. Wash. 2011).

[17] *Preventive Med. Assocs., Inc. v. Commonwealth*, 992 N.E.2d 257, 273 (Mass. 2013) ("[T]he judge or officer issuing the search warrant likely does not have the technical expertise to assess the propriety of a particular forensic analysis.").

[18] *United States v. Galpin*, 720 F.3d 436, 477 (2d Cir. 2013); *United States v. Stabile*, 633 F.3d 219, 234 (3d Cir. 2011); *Bonner*, 2013 WL 3829404, at *19. As this report was in final review, NACDL learned of a proposed amendment to Fed. R. Crim. P. 41, which would authorize warrants to gain remote access to devices in districts other than the issuing district, including access to the services the device has connected to, like "the cloud." *See*, Materials for Advisory Comm. on Criminal Rules Meeting 165, http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Agenda%20Books/Criminal/CR2014-04.pdf (Apr. 7-8, 2014).

[19] *Galpin*, 720 F.3d at 447.

[20] Digital devices may, for example, contain booby traps, inaccessible files, passwords, and encryption. *CDT*, *supra* note 15, at 1167-68. Even where suspects have not intentionally obfuscated data, computers contain a wealth of information, the entirety of which only trained experts can uncover.

[21] *United States v. Johnston*, No. CR. S–07–00425KJM, 2012 WL 1292457, at *6 (E.D. Cal. Apr. 16, 2012); *see United States v. Widner*, No. 09–CR–6225L, 2010 WL 4861513 (W.D.N.Y. Aug. 20, 2010).

[22] *CDT*, *supra* note 15 ; *In re Appeal of Application for Search Warrant*, 71 A.3d 1158 (Vt. 2012); *see Bonner*, 2013 WL 3829404, at *19; *Smallwood*, 113 So.3d at 732.

[23] *United States v. Burgess*, 576 F.3d 1078, 1094 (10th Cir. 2009) (It would be "folly for a search warrant to attempt to structure the mechanics of the search" because "imposing such limits would unduly restrict legitimate search objectives."); *United States v. Grimmett*, 439 F.3d 1263, 1270 (10th Cir. 2006) ("[A] computer search 'may be as extensive as reasonably required to locate the items described on the warrant'"); *Bizewski*, 2013 WL 1849282, at *13.

[24] *See* Orin Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241, 1242 (2010).

[25] *See, e.g.*, James Saylor, *Computers as Castles: Preventing the Plain View Doctrine from Becoming a Vehicle for Overbroad Digital Searches*, 79 FORDHAM L. REV. 2809 (2011).

[26] *See, e.g.*, *Muehler v. Mena*, 544 U.S. 93, 100 (2005); *United States v. Lopez-Cruz*, 730 F.3d 803, 810 (9th Cir. 2013); *United States v. Christie*, 717 F.3d 1156, 1166 (10th Cir. 2013); *see also* Fed. R. Crim. P. 41. While Rule 41 expressly authorizes warrants for seizure of data, presently, it is devoid of any substantive guidance concerning the scope of warrants or their means of execution.

[27] In addition to the sources cited in this report, *see* Jeffrey Bellin, *Crime-Severity Distinctions and the Fourth Amendment: Reassessing Reasonableness in a Changing World*, 97 Iowa L. Rev. 1, 42 (2011); Andy Boulton, *E-Discovery Rules and the Plain View Doctrine: The Scylla and Charybdis of Electronic Document Retention*, 37 J. Corp. L. 435, 440 (2012); Donald A. Dripps, *"Dearest Property": Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure*, 103 J. Crim. L. & Criminology 49, 57 (2013); Stephen Guzzi, *Digital Searches and the Fourth Amendment: The Interplay Between the Plain View Doctrine and Search-Protocol Warrant Restrictions*, 49 Am. Crim. L. Rev. 301, 304 (2012); Stephan E. Henderson, *What Alex Kozinski and the Investigation of Earl Bradley Teach About Searching and Seizing Computers and the Dangers of Inevitable Discovery*, 19 Widener L. Rev. 115 (2013); Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 Va. L. Rev. In Brief 1, 3 (2011); Kaitlyn R. O'Leary, *What the Founders Did No See Coming: The Fourth Amendment, Digital Evidence, and the Plain View Doctrine*, 46 Suffolk U. L. Rev. 211, 230 (2013); Christina M. Schuck, *A Search for the Caselaw to Support the Computer Search "Guidance" in United States v. Comprehensive Drug Testing*, 16 Lewis & Clark L. Rev. 741 (2012); Mark B. Sheppard & Erin C. Dougherty, *"Tapping" Into Wall Street*, 26-WTR Crim. Just. 20, 26 (2012); Christopher Slobogin, *Why Crime Severity Analysis is Not Reasonable*, 97 Iowa L. Rev. Bull. 1, 7 (2012); Mark Wilson, *Castle in the Cloud: Modernizing Constitutional Protections for Cloud-Stored Data on Mobile Devices*, 43 Golden Gate U. L. Rev. 261, 279-80 (2013).

[28] *CDT*, *supra* note 15, at 1166.

[29] *Id*.

[30] *Id*.

[31] *Id*. at 1167.

[32] *Id*.

[33] *Id*. at 1175.

[34] *United States v. Comprehensive Drug Testing, Inc.*, 513 F.3d 1085, 1092 (9th Cir. 2008) (Government threatened to "seize all computer equipment for up to sixty days," which would shut the CDT business down).

[35] *CDT*, *supra* note 15, at 1168.

[36] *Id*.

[37] *United States v. Tamura*, 694 F.2d 591 (9th[t] Cir. 1982).

[38] *CDT*, *supra* note 15, at 1168.

[39] *Id*. at 1169.

[40] *Id*. at 1170-71 ("If the government can't be sure whether data may be concealed, compressed, erased or booby-trapped without carefully examining the contents of every file . . . then everything the government chooses to seize will, under this theory, automatically come into plain view.").

[41] *Id*. at 1171.

[42] *Id*.

[43] *Coolidge v. New Hampshire*, 403 U.S. 443, 469-70 (1971).

[44] *Id*. at 470.

[45] *Horton v. California*, 496 U.S. 128, 137 (1990). *Compare Frasier v. State*, 794 N.E.2d 449, 461 (Ind. Ct. App. 2003) (retaining the inadvertence requirement).

[46] *Horton*, 496 U.S. at 136.

[47] There are limits to this. If, post-search, it is unreasonable to believe that evidence of the crime for which a warrant issued would not be located where agents searched, the evidence therein seized should be suppressed. *See United States v. Kim*, 677 F. Supp. 2d 930, 945, 949-50 (S.D. Tex. 2009) (holding search of file labeled "Illegal_Loli#" during a warranted search for Computer Intrusion unreasonable in part because only the "World's Dumbest Criminal[]" would hide evidence of crime by labeling it to be indicative of a more serious crime.).

[48] *CDT*, *supra* note 15, at 1174.

[49] *Id*. at 1170-71, 1177.

[50] *Id*. at 1180-81 (Bea, J., concurring in part and dissenting in part) ("Here, the portion of the spreadsheet . . . that contained the drug testing results, contained both the names of the ten ballplayers who were the subjects of the warrant and the names of many other ballplayers, the records of whom the government did not have probable cause to search and seize. The spreadsheet did not, however, initially display on the agent's computer screen the results of steroid testing as to the other ballplayers. To see the spreadsheet column containing the results of the tests of the other ballplayers, the agent had to scroll to his right on the spreadsheet, onto another screen. However, once he scrolled to the right, the agent could see not only the testing results for the targeted ten, but also the results for all of the other ballplayers whose results were listed on the spreadsheet. A valid "plain view" seizure of items that are truly "immediately apparent" would have required the agent to display only the testing results for the ballplayers for whom he had a warrant, and seize only evidence of additional illegality if such evidence is "immediately apparent" as part of the segregated results for those ballplayers. For instance, the agent could have selected the spreadsheet rows for the ten ballplayers for whom he had a warrant, then copied and pasted those rows into a blank spreadsheet. If he had done so, he would have seen only those drug testing results for which he had a warrant.").

[51] *Id*. at 1178 (Kozinski, C.J., concurring).

[52] *Id*. at 1180.

[53] *In re Appeal of Application for Search Warrant*, 71 A.3d at 1171.

[54] *See Burgess*, 576 F.3d at 1094 ("A warrant may permit only the search of particularly described places and only particularly described things may be seized. As the description of such places and things becomes more general, the method by which the search is executed become [sic] more important—the search method must be tailored to meet allowed ends. And those limits must be functional."); *United States v. Lacy*, 119 F.3d 742, 746 (9th Cir. 1997) (warrant without limiting protocols) ("[T]his type of generic classification is acceptable 'when a more precise description is not possible,' . . . and in this case no more specific description of the computer equipment sought was possible."); *In re Search of 3817 W. West End*, 321 F. Supp. 2d 953, 960 (N.D. Ill. 2004) ("[G]eneric classifications in a warrant are acceptable only when a more precise description is not possible." (quoting *United States v. Kow*, 58 F.3d 423, 427 (9th Cir. 1995))).

[55] *Horton*, 496 U.S. at 135.

[56] *Minnesota v. Dickerson*, 508 U.S. 366, 375 (1993).

[57] *Arizona v. Hicks*, 480 U.S. 321, 326-27 (1987).

[58] *Horton*, 496 U.S. at 134; *Coolidge*, 403 U.S. at 465.

[59] *Horton*, 496 U.S. at 136 ("[T]he 'plain view' doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges."); *Coolidge*, 403 U.S. at 466 (same).

[60] *See, e.g., Georgia v. Randolph*, 547 U.S. 103, 137 (2006) ("The normal Fourth Amendment rule is that items discovered in plain view are admissible if the officers were legitimately on the premises.").

[61] *United States v. Williams*, 592 F.3d 511, 522 (4th Cir. 2010) (emphasis in original) (citing *Maryland v. Garrison*, 480 U.S. 79, 84 (1987)).

[62] *Coolidge*, 403 U.S. at 467.

[63] *Id*.

[64] *See United States v. Farlow*, 681 F.3d 15 (1st Cir. 2012); *United States v. Stabile*, 633 F.3d 219, 240-41 (3d Cir. 2011); *United States v. Williams*, 592 F.3d 511, 521-22 (4th Cir. 2010).

[65] *United States v. Mann*, 592 F.3d 779, 786 (7th Cir. 2010) ("[W]e simply counsel officers and others involved in searches of digital media 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. As discussed above, with the exception of the four "KFF Alert" images, Detective Huff's search was indeed targeted to uncovering evidence of voyeurism as described in what Mann now concedes was a lawful warrant. In so doing, he uncovered obvious evidence of child pornography. Although we now hold that his actions were within the scope of the warrant, we emphasize that his failure to stop his search and request a separate warrant for child pornography is troubling."); *Burgess*, 576 F.3d at 1092 ("As in this case, the officer in [*United States v. Carey*] inadvertently discovered an image of child pornography while searching for electronic evidence of drug activity. After opening the first file, the officer in *Carey* temporarily abandoned the search for drug evidence and proceeded to look through the hard drive for more images of child pornography. We determined the extension of the search to locate further evidence of child pornography exceeded the scope of the warrant authorizing a search for evidence of drug crimes. Here Hughes immediately stopped the preview upon seeing an instance of suspected child pornography and obtained another warrant to search for pornography."); *Walser*, 275 F.3d at 986-87; *Carey*, 172 F.3d at 1275 (intermingled documents) ("[L]aw enforcement must engage in the intermediate step of sorting various types of documents and then only search the ones specified in a warrant. Where officers come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, the officers may seal or hold the documents pending approval by a magistrate of the conditions and limitations on a further search through the documents.").

[66] *In re Appeal of Application for Search Warrant*, 71 A.3d at 1174.

[67] *CDT*, *supra* note 15, at 1180.

[68] *Galpin*, 720 F.3d at 451 ("[T]he district court's review of the plain view issue should take into account the degree, if any, to which digital search protocols target information outside the scope of the valid portion of the warrant. To the extent such search methods are used, the plain view exception is not available."); *United States v. Miranda*, 325 Fed.Appx. 858, 860 (11th Cir. 2009); *Bonner*, 2013 WL 3829404, at *19 ("The process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect.") (quoting *CDT*, *supra* note 15, at 1177).

[69] *United States v. Giberson*, 527 F.3d 882, 890 (9th Cir. 2008); *Ohio v. McCrory*, No. 2009CR0259, 2011 WL 382757, at *2 (Ohio Ct. App. 2011); *Rosa v. Commonwealth*, 628 S.E.2d 92, 98, 101 (Va. Ct. App. 2006); *Wisconsin v. Schroeder*, 613 N.W.2d 911, 913, 916 (Wis. Ct. App. 2000).

[70] *Carey*, 172 F.3d at 1276; *Kim*, 677 F. Supp. 2d 930.

[71] *In re Appeal of Application for Search Warrant*, 71 A.3d at 1179.

[72] *Preventive Med. Assocs.*, 992 N.E.2d at 260, 272.

[73] *In re: Grand Jury Subpoenas*, 454 F.3d 511, 524 (6th Cir. 2006) (Mandating that a Special Master conduct an initial review of materials).

[74] *Bonner*, 2013 WL 3829404, at 19.

[75] *Schreiber v. Schreiber*, 904 N.Y.S.2d 886 (N.Y. Sup. Ct. 2010) ("Outside the matrimonial context, courts have been loathe to sanction an intrusive examination of an opponent's computer hard disk drive as a matter of course."); *Bennett v. Martin*, 928

N.E.2d 763, 773-74 (Ohio Ct. App. 2009) ("Generally, courts are reluctant to compel forensic imaging, largely due to the risk that the imaging will improperly expose privileged and confidential material contained on the hard drive. Because allowing direct access to a responding party's electronic information system raises issues of privacy and confidentiality, courts must guard against undue intrusiveness.").

[76] *Bennett*, 928 N.E.2d at 775-76 ("[C]ourts [usually] adopt a protocol whereby an independent computer expert, subject to a confidentiality order, creates a forensic image of the computer system. The expert then retrieves any responsive files (including deleted files) from the forensic image, normally using search terms submitted by the plaintiff. The defendant's counsel reviews the responsive files for privilege, creates a privilege log, and turns over the nonprivileged files and privilege log to the plaintiff."); *see Schreiber*, 904 N.Y.S.2d at 893 (the court permitted a search of a hard drive, "subject to the following protocol: the attorney will select its own computer expert; the expert will search, copy, print, and deliver to the court in a sealed envelope the relevant portions of the documents from his hard disk drive; the attorney will have ten days after delivery within which to object to the production of the documents to the parties' attorneys; the merit of any objections raised will be determined by the court; if no objections are timely raised by the attorney, paper copies of such documents will be delivered to the parties' attorneys.") (citing Matter of Maura, 842 N.Y.S.2d 851, 180-81 (N.Y. Sup. Ct. 2007)); *Etzion v. Etzion*, 796 N.Y.S.2d 844 (N.Y. Sup. Ct. 2005) (Mirroring permitted, but use of a discovery "referee" required).

[77] *In re Appeal of Application for Search Warrant*, 71 A.3d at 1173-74.

[78] *Preventive Med. Assocs.*, 992 N.E.2d at 271.

[79] *Galpin*, 720 F.3d at 451; *United States v. Schesso*, 730 F.3d 1040, 1050 (9th Cir. 2013); *United States v. Hill*, 459 F.3d 966, 978 (9th Cir. 2006); *United States v. Nazemzadeh*, No. 11–cr–5726–L, 2013 WL 544054, at *5 (S.D.Cal. 2013); In re *Search of W. West End*, 321 F. Supp. 2d 953, 961 (N.D. Ill. 2004).

[80] *Bonner*, 2013 WL 3829404, at *17.

[81] *In re Appeal of Application for Search Warrant*, 71 A.3d at 1162.

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

[83] *Preventive Med. Assocs.*, 992 N.E.2d 257, 830 (2013) ("Advance approval for the particular methods to be used in the forensic examination of the computers is not necessary . . . Indeed, the judge or officer issuing the search warrant likely does not have the technical expertise to assess the propriety of a particular forensic analysis."); *see also Bizewski*, 2013 WL 1849282, at *13.

[84] *Schesso*, 730 F.3d at 1050; *United States v. Burdulis*, No. 10–40003(FDS), 2011 WL 1898941, at *7 (D.Mass. 2011).

[85] *CDT*, *supra* note 15, at 1179.

[86] *Id*. at 1180.

[87] *See* Fed. R. Crim. P. 41(c); *see also DOJ Manual* at 63.

[88] *Id*. at 75.

[89] *Id*. at 72-73.

[90] *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989, 1006-07 (9th Cir. 2009).

[91] *CDT*, *supra* note 15, at 1180.

[92] *Schesso*, 730 F.3d at 1050 ("[J]udges may consider such protocols or a variation on those protocols as appropriate in electronic searches."). The proper balance between law enforcement and rights to privacy will be made "on a case-by-case basis."

[93] *CDT*, *supra* note 15, at 1179.

[94] *Id*.

[95] Agents often already perform such careful searches. *See Walser*, 275 F.3d at 984-85; *McCrory*, 2011 WL 382757, at *2; *Rosa*, 628 S.E.2d at 98; *Schroeder*, 613 N.W.2d at 914.