NOTES & COMMENTS

A SEARCH FOR THE CASELAW TO SUPPORT THE COMPUTER SEARCH "GUIDANCE" IN *UNITED STATES V. COMPREHENSIVE DRUG TESTING*

by
Christina M. Schuck[*]

The ubiquitous use of computers by individuals and businesses presents a unique challenge to courts attempting to balance the legitimate needs of law enforcement with individuals' Fourth Amendment rights. Despite a recent failed attempt by the Ninth Circuit in United States v. Comprehensive Drug Testing *(*CDT*) to take a special approach to computer searches, it is still possible for courts to establish guidelines that are both supportable and practical.*

Using the CDT *guidelines, courts going forward should: (1) ask the government to forswear the use of the plain view doctrine to prevent a search of electronic data from becoming a prohibited general search; (2) narrowly apply the use of segregation teams in cases where third party information is at risk; (3) only require a search protocol in very limited situations; and (4) require the government to disclose the actual risks to data destruction in the particular case, instead of relying on generic hazards to justify a broad seizure of data.*

Although unsupported in the opinion, the CDT *guidelines provide courts valuable tools to analyze the reasonableness of a computer search.*

[*] J.D. 2011 Lewis & Clark Law School. Special thanks to Professor Toni Berres-Paul, David Angeli, and Matt Sasson.

I. INTRODUCTION

Courts and commentators agree that the Fourth Amendment's prohibition of general warrants limits computer searches, but disagree on how to prevent them from becoming the general searches feared and loathed by the Framers. Some courts hint that a special approach may be necessary for computer searches; others eschew any heightened protection. Some circuits compare computers to containers; others analogize computers to briefcases, file cabinets, warehouses or intermingled paper documents. The confusing array of analogies and disagreement between courts produces conflicting results that hamper law enforcement efforts and endanger individuals' Fourth Amendment protections.

Amidst this confusion, in the 2009 en banc opinion, *United States v. Comprehensive Drug Testing, Inc.* (*CDT*)[1], the Ninth Circuit attempted to draw a clear line in the sand. In order to strike the "right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures," the court laid out the following five guidelines: (1) magistrates should insist that the government waive reliance upon the plain view doctrine in digital evidence cases; (2) specialized personnel or an independent third party must segregate and redact the data; (3) warrants and subpoenas must disclose the actual risks of destruction of evidence; (4) the government must design a search protocol to uncover only the information for which probable cause exists; and (5) the government must destroy or return non-responsive data.[2] Unfortunately, although attempting to serve everyone's interest by defining clear rules, Chief Judge Alex Kozinski's opinion announced new rules for computer searches without much support.[3]

Swift reaction to *CDT* ensued. Commentators called the decision an "earthquake"[4] and a "blockbuster computer search and seizure decision."[5] The government responded to the opinion by requesting an unprecedented full en banc rehearing,[6] claiming that "judges are following [*CDT*'s] guidelines—to calamitous effect,"[7] with computer searches grinding to a complete halt in some districts and delayed or impeded throughout the Ninth Circuit.[8] A year later, the Ninth Circuit issued a revised opinion, per curiam, "constitut[ing] the final action of the court" and declaring no petitions for rehearing would be

[1] United States v. Comprehensive Drug Testing, Inc. (*CDT En Banc*), 579 F.3d 989 (9th Cir. 2009) (en banc), *revised and superseded by* 621 F.3d 1162 (9th Cir. 2010) (en banc) (per curiam).

[2] *Id.* at 1006.

[3] *See id.* at 1012–14 (Callahan, J., concurring in part and dissenting in part) (warning that the majority's guidelines are overbroad, unduly restrictive on law enforcement, and without legal authority).

[4] Susan Brenner, *Earthquake*, CYB3RCRIM3 (Aug. 29, 2009, 3:33 PM), http://cyb3rcrim3.blogspot.com/2009/08/earthquake.html (noting that the decision is going to "shake things up" within the cybercrime realm); *see also* Orin Kerr, *Ninth Circuit Enacts* Miranda*-Like Code for Computer Search and Seizure*, VOLOKH CONSPIRACY (Aug. 26, 2009, 1:38:PM), http://volokh.com/archives/archive_2009_08_23-2009_08_29.shtml#1251308337 ("I can't recall having read anything quite like it, although it does bring to mind *Miranda v. Arizona*.").

[5] Orin Kerr, *Ninth Circuit Considers Super-En-Banc for* Comprehensive Drug Testing, VOLOKH CONSPIRACY (Nov. 5, 2009, 5:39 PM), http://volokh.com/2009/11/05/ninth-circuit-considers-super-en-banc-for-comprehensive-drug-testing/.

[6] Brief for the United States in Support of Rehearing En Banc by the Full Court at 2, United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989 (9th Cir. 2009) (Nos. 05-10067, 05-15006, 05-55354) [hereinafter CDT Appellant Brief].

[7] Shane Harris, *Cuffing Digital Detectives*, NAT'L JOURNAL, http://www.nationaljournal.com/njmagazine/id_20091219_3389.php (last updated Jan. 31, 2011, 8:37 AM).

[8] CDT Appellant Brief, *supra* note 6, at 1.

considered.[9] The revised opinion removed the binding guidelines set forth in the original en banc opinion and they now exist only in Judge Kozinski's concurrence as "guidance."[10]

Nevertheless, the guidelines proposed by Judge Kozinski and joined by four other judges,[11] still remain a bold approach to computer searches and an unprecedented attempt to create bright-line rules to protect individuals' Fourth Amendment rights. With this in mind, this Note examines *CDT*'s guidelines within the context of current case law to determine if they are supportable. It also explores the practicality of the guidelines, including how they work together and if they are all necessary. Part II summarizes the facts and holdings of *CDT*. Part III explains the difficulties of computer searches. Part IV discusses the Fourth Amendment rights of individuals. Part V analyzes *CDT*'s guidelines, critically examining both their support and lack thereof. Finally, Part VI proposes a solution for employing the guidelines going forward.

II. AN OVERVIEW OF *CDT*

The facts of *CDT* provided the ideal background for a bold new approach to computer searches in criminal investigations. *CDT* differs from other computer search cases in three important respects. First, this case did not involve investigators searching a suspect's computer for evidence of a crime like drug dealing or tax fraud. Instead, investigators searched the computer system of a legitimate business not suspected of any wrongdoing and in the process exposed the confidential information of hundreds of innocent parties.[12] Second, the computer search did not reveal evidence of a different, particularly abhorrent crime, like child pornography.[13] Third, the information sought in *CDT* was discrete and easily located employing a straightforward search protocol.[14]

The litigation in *CDT* began in 2002, following a Major League Baseball (MLB) Players Association collective bargaining agreement which consented to the testing for banned substances.[15] Comprehensive Drug Testing, Inc. (CDT, Inc.) collected the specimens from the players, and the laboratory, Quest Diagnostics, Inc., (Quest) performed the

[9] United States v. Comprehensive Drug Testing, Inc. (*CDT Per Curiam*), 621 F.3d 1162, 1165 (9th Cir. 2010) (en banc) (per curiam).

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

[11] Joining the concurrence are Judges Kleinfeld, W. Fletcher, Paez, and M. Smith. *Id.*

[12] *CDT En Banc*, 579 F.3d 989, 1005 (9th Cir. 2009).

[13] *See* Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L.J. 193, 200 (2005) (stating child pornography and sexual exploitation of children make up a "shockingly large percentage of the decided cases").

[14] United States v. Comprehensive Drug Testing, Inc. (*CDT Panel*), 513 F.3d 1085, 1120 (9th Cir. 2008), *modified on reh'g en banc*, 579 F.3d 989 (9th Cir. 2009).

[15] *CDT En Banc*, 579 F.3d at 993.

tests.[16] CDT, Inc. maintained a list of the players and their test results and Quest kept the actual specimens.[17] The league guaranteed MLB players anonymity and confidentiality in the testing.[18] That same year, the federal government began investigating Bay Area Laboratory Cooperative (BALCO) for providing steroids to professional baseball players.[19] During this investigation, the government subpoenaed all MLB drug testing records and specimens from CDT, Inc. and Quest.[20] Unable to reach a compliance agreement, CDT, Inc. and the MLB Players moved to quash the subpoena.[21] Importantly, during the dispute over the scope of the subpoena, CDT, Inc. and Quest promised not to destroy or alter any of the data in question.[22]

A. The Warrant to Search CDT, Inc.

The same day the motion to quash was filed, the government applied for a warrant in the Central District of California to search CDT, Inc.'s facilities.[23] The warrant authorized the seizure of the drug testing records for ten named MLB players and the search of computer equipment and storage devices.[24] In addition, the warrant provided for a seizure of a copy of all data or computer equipment itself in the event an on-site search was impracticable.[25] The affidavit in support of the search warrant, in an attempt to justify a broad seizure of computer records, explained some general hazards of retrieving electronically stored data.[26] In particular, the government explained that data may be erased, hidden, encrypted, or disguised ingeniously by giving files misleading names.[27] The government also cautioned that "booby traps" could be set up to destroy or alter data if certain procedures were not scrupulously followed.[28]

The magistrate judge, although persuaded by the government's case for a blanket seizure and off-site examination of the evidence, imposed conditions upon the warrant's execution. Specifically, the warrant specified that if seizure of all data or equipment was necessary, "computer personnel," and not the case agents, would review the data,

[16] *Id.*
[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] *CDT Panel*, 513 F.3d 1085, 1090 (9th Cir. 2008).
[21] *CDT En Banc*, 579 F.3d at 993.
[22] *CDT Panel*, 513 F.3d at 1090.
[23] *CDT En Banc*, 579 F.3d at 993. That same day, the government also secured a warrant in the District of Nevada to search Quest. *Id.*; *CDT Panel*, 513 F.3d at 1090–91.
[24] *CDT Panel*, 513 F.3d at 1091–92.
[25] *Id.*
[26] *CDT En Banc*, 579 F.3d at 995.
[27] *Id.*
[28] *Id.*

retaining the evidence authorized by the warrant and designating the remainder for return within a reasonable amount of time.[29]

B. The Execution of the Warrant

On April 8, 2004, twelve agents, including a computer forensic expert, executed the search warrant.[30] During the raid, the agents seized the records not only of the players listed in the warrant, but also the records of hundreds of other professional athletes—none of whom were suspected of any wrongdoing.[31] Initially, CDT, Inc. personnel resisted and did not cooperate with agents.[32] However, later in the day, a CDT, Inc. director offered the agents a document containing only the test results for the ten named players listed in the search warrant.[33] The agents refused and continued their search. Finally, a director identified the "Tracey Directory," a computer directory containing all of the computer files for CDT, Inc.'s professional sports drug testing programs.[34] Following the recommendation of the computer forensic expert, the agents seized the entire Tracey Directory, despite CDT, Inc. personnel showing them a subdirectory containing only MLB players.[35] Even though the government possessed probable cause for only ten MLB players, the agents seized numerous subdirectories and hundreds of files outside the scope of the warrant.[36] Notwithstanding language in the warrant limiting the initial review and segregation of the data to computer personnel, the case agent personally reviewed the seized files within the Tracey Directory.[37]

C. The Fallout

On May 5, 2004, based upon the information in the Tracey Directory, the government obtained new search warrants to seize all

[29] *Id.* at 999. The dissenting judges dispute that the warrant required the initial review of the data to be completed by a computer specialist. *Id.* at 1011 (Callahan, J., concurring in part and dissenting in part) (citing *CDT Panel*, 513 F.3d at 1111).

[30] *CDT Panel*, 513 F.3d at 1092.

[31] *See id.* at 1092–93.

[32] *Id.* at 1092.

[33] *Id.*

[34] *Id.*

[35] *Id.* at 1092–93; *id.* at 1134 (Thomas, J., concurring in part and dissenting in part).

[36] *Id.* at 1136; *CDT En Banc*, 579 F.3d 989, 1005 (9th Cir. 2009). The Tracey Directory contained 2,911 files, which included the drug testing records of hundreds of MLB players, thirteen other sports organizations, three unrelated sporting competitions and even three non-sports business entities. *CDT Panel*, 513 F.3d at 1117; *id.* at 1145–46 (Thomas, J., concurring in part and dissenting in part).

[37] *CDT Panel*, 513 F.3d at 1093. Judge Bea remarked how easy it would have been for Agent Novitsky not to have examined the testing information on the players outside of the scope of the warrant. *CDT En Banc*, 579 F.3d at 1016 n.2 (Bea, J. concurring in part and dissenting in part).

specimens and records pertaining to over one hundred non-BALCO players who had tested positive for steroids.[38] The names of some of these players were leaked to the media.[39] In response, CDT, Inc. and the MLB Players Association filed three motions in three different districts: two Federal Rule of Criminal Procedure 41(g)[40] motions to return the property seized under the warrants, and one motion to quash the subpoenas.[41] Three separate district court judges not only granted the motions, but expressed "grave dissatisfaction" with the government's conduct, with one of the judges reportedly asking, "What happened to the Fourth Amendment? Was it repealed somehow?"[42] Judge Cooper in the Central District of California ordered the return of the Tracey Directory to CDT, Inc. based upon the government's noncompliance with the procedures specified in the warrant, concluding the government's actions displayed a "callous disregard for the rights of third parties."[43] Judge Mahan in Nevada also ordered the government to return the property, except for the files pertaining to the ten players specified within the warrant.[44] Additionally, Judge Illston quashed the May 6, 2004 subpoena.[45]

The government appealed all three orders and a three-judge panel of the Ninth Circuit reversed Judge Mahan's and Judge Illston's decisions to quash the subpoenas, but determined Judge Cooper's ruling had not been timely appealed.[46] The Ninth Circuit voted to rehear the case en banc and upheld the three district courts' rulings that the government had unlawfully seized the electronic spreadsheet from CDT, Inc.[47] The *CDT* en banc opinion, however, functioned as much more than "another round in the battle between [CDT, Inc.] and the federal government."[48]

---

[38] *CDT Panel*, 513 F.3d at 1094.

[39] The most famous MLB name leaked was Alex Rodriguez. *See* Selena Roberts & David Epstein, *Sources Tell SI Alex Rodriguez Tested Positive for Steroids in 2003*, SI.COM (Feb. 7, 2009, 10:12 AM), http://sportsillustrated.cnn.com/2009/baseball/mlb/02/07/alex-rodriguez-steroids/; Michael Horowitz et al., *The Blurring of Plain View*, WHITE-COLLAR CRIME, Nov. 2009, at 1, 2.

[40] FED. R. CRIM. P. 41 (g) ("Motion to Return Property[:] A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return. The motion must be filed in the district where the property was seized. The court must receive evidence on any factual issue necessary to decide the motion. If it grants the motion, the court must return the property to the movant, but may impose reasonable conditions to protect access to the property and its use in later proceedings.").

[41] *CDT En Banc*, 579 F.3d at 993–94.

[42] *Id.* at 994; *CDT Panel*, 513 F.3d 1085, 1116 (9th Cir. 2008).

[43] *CDT En Banc*, 579 F.3d at 995.

[44] *Id.* at 994.

[45] *CDT Panel*, 513 F.3d at 1095.

[46] *Id.* at 1089–90, 1097–98, 1116.

[47] *CDT En Banc*, 579 F.3d at 994, 1007.

[48] Susan W. Brenner, *Internet Law in the Courts: New Ninth Circuit Ruling Has Major Implications for Digital Search and Seizure*, J. INTERNET L., Oct. 2009, at 18, 18.

Rather, the Ninth Circuit appeared to use the original en banc opinion to address issues that "had presumably been troubling the judges for some time."[49] Although the guidelines are no longer binding, in his concurrence, Judge Kozinski emphasized their importance and usefulness in providing guidance to "offer[] the government a safe harbor, while protecting the people's right to privacy."[50]

III. THE DIFFICULTIES OF COMPUTER SEARCHES

A. The Quantity and Quality of Electronic Data

For well over a decade, courts have struggled within the digital data context to balance law enforcement's legitimate need to collect and examine evidence with individuals' Fourth Amendment rights against unreasonable searches and seizures. The struggle begins with the amount and nature of digital data. Computers contain an incomprehensible amount of information. People and businesses use computers as much more than file cabinets; they also utilize computers as telephones, diaries, photo albums, stereos, and televisions.[51] As a result, computers function as "a stash of child porn, a file cabinet full of counterfeit checks, a weapon for attacking an electric power grid, or a record of a drug conspiracy and money laundering operation."[52]

With their increasing prevalence in our daily lives and the amount of information stored, computers are an invaluable source of evidence to criminal investigators. Not only do users store information on a computer's internal hard drive, they also save data to external storage devices including CDs, DVDs, thumb drives, or external hard drives.[53] In addition to the data computer users deliberately save, the computer's operating system creates and stores a wealth of information users are often unaware of.[54] Applications and programs, particularly web browsers, store information on the user's interests, identity, and habits.[55]

---

[49] *Id.*

[50] *CDT Per Curiam*, 621 F.3d 1162, 1178 (9th Cir. 2010) (Kozinski, J., concurring).

[51] David H. Angeli et al., *The Plain View Doctrine and Computer Searches: Balancing Law Enforcement's Investigatory Needs with Privacy Rights in the Digital Age*, CHAMPION, Aug. 2010, at 18, 19; *see also, e.g.*, MICHELE C.S. LANGE & KRISTIN M. NIMSGER, ELECTRONIC EVIDENCE AND DISCOVERY: WHAT EVERY LAWYER SHOULD KNOW *NOW* 208 (2d ed. 2009); Samantha Trepel, *Digital Searches, General Warrants, and the Case for the Courts*, 10 YALE J.L. & TECH. 120, 128 (2007).

[52] Terrence Berg, *Practical Issues in Searching and Seizing Computers*, 7 T.M. COOLEY J. PRAC. & CLINICAL L. 27, 33 n.12 (2004).

[53] Angeli et al., *supra* note 51, at 19.

[54] 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 (3d ed. 2009) [hereinafter DOJ MANUAL], *available at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.

[55] Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 543 (2005). An application is "why you use a computer in the first place," allowing users to

Additionally, operating systems, such as Microsoft Windows, record information such as internet usage, attachment of flash drives, and times the computer was in use.[56] This information, called metadata, also reveals what files have been created or edited and even how the file was edited.[57] Thus, data stored on a computer can reveal who has used the computer, when, and how.[58]

Courts also struggle with the nature of digital evidence. Unless the computer is stolen and contraband itself, the evidence a computer provides—such as digital images or source code—is not physical, like a bag of cocaine or stolen jewelry.[59] Rather, at its most basic level, all electronic data "is simply a collection of ones and zeros organized into groups"[60] requiring a machine and programs to organize it into something meaningful. The most common group is a string of eight zeros and ones called a byte.[61] Bytes are then organized into clusters, which are the smallest group or collection at the software level, typically comprised of four or thirty-two kilobytes.[62] A computer file, such as a Microsoft Excel spreadsheet, spans multiple clusters. Once any part of a cluster is used, the operating system marks the entire cluster as unavailable to store additional data.[63] The computer's operating system tracks which clusters are currently in use and which ones are available to store data.[64]

The computer's operating system serves important functions. Most importantly, it organizes the underlying ones and zeros into files and folders users are familiar with.[65] The operating system also maintains a file system that tracks where the data is located on a hard drive.[66] To do so, the file system creates a file allocation table telling the operating

balance checkbooks, view movies, or produce documents. CHRIS DAVIS ET AL., HACKING EXPOSED: COMPUTER FORENSICS SECRETS & SOLUTIONS 25 (2005). Common programs include software like Microsoft Word or Excel. Common web browsers include Mozilla FireFox or Internet Explorer.

[56] DOJ MANUAL, *supra* note 54, at 62.

[57] *Id.*

[58] *Id.*; Kerr, *supra* note 55, at 543. One famous example occurred in 2006, when AOL publicized the search histories of more than 650,000 of its users. Although AOL did not include names or user identities, the search terms revealed a great deal of information about the users. Declan McCullagh, *AOL's Disturbing Glimpse into Users' Lives*, CNET, (Aug. 7, 2006, 8:05 PM), http://news.cnet.com/2100-1030_3-6103098.html.

[59] 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, 1071 (2007).

[60] *Id.* at 1091 (footnote omitted).

[61] Kerr, *supra* note 55, at 538–39.

[62] *Id.* at 539.

[63] McLain, *supra* note 59, at 1092.

[64] *Id.*

[65] Wayne Jekot, *Computer Forensics, Search Strategies, and the Particularity Requirement*, 7 PITT. J. TECH. L. & POL'Y, Spring 2007, Art. 5, at *5, http://tlp.law.pitt.edu/wp-content/uploads/2009/10/Vol_12_Jekot.pdf.

[66] *Id.* at *6; DAVIS ET AL., *supra* note 55, at 113; Kerr, *supra* note 55, at 539–40.

system where to find a file.[67] When a user deletes a file, the file allocation table entry is deleted, but the underlying data remains because the clusters comprising the file are simply redesignated as available to store data.[68] Therefore, if the cluster is not overwritten, the data it holds is recoverable using forensic software.[69] Significantly, even when a file cannot be recovered in its entirety, fragments of the file often still exist.[70]

The file system also controls the internal headers of files which identify what type of file it is. Accordingly, the file type is controlled by the system, not by what the user calls the file.[71] To illustrate, although a user can save a word processing document with an image file extension, by naming a letter "BBQ.jpg," the internal header would still identify the file as a word processing document.[72] When a computer is searched pursuant to a warrant, all of this data potentially becomes available to investigators.

B. Searching Computers and Other Electronic Storage Devices

The phrase "computer forensics" describes the "acquisition, preservation, and analysis of electronically stored information . . . in such a way that ensures its admissibility for use as either evidence, exhibits, or demonstratives in a court of law."[73] Thus, there are three important parts to any computer search: data acquisition, preservation, and reduction.[74] Investigators must first acquire data, for example from a hard drive, or as in *CDT*, the Tracey Directory.[75] Next, investigators preserve the data by creating a "mirror image" or "bitstream" copy of the storage device in a read-only format in order to ensure the integrity of the electronic evidence.[76] Finally, investigators search through the data, separating the responsive from the non-responsive data.

The DOJ Manual instructs that, except in limited situations, a computer's hard drive should not be searched on-site because it is too time-consuming.[77] Instead, the Manual recommends that the search

---

[67] DAVIS ET AL., *supra* note 55, at 113–14.

[68] *Id.* at 118; Jekot, *supra* note 65, at *6.

[69] DAVIS ET AL., *supra* note 55, at 118; Kerr, *supra* note 55, at 542.

[70] DAVIS ET AL., *supra* note 55, at 119.

[71] LANGE & NIMSGER, *supra* note 51, at 234 figs.5.6 & 5.7 (giving examples of an operating system and a word processing document's different metadata).

[72] *Id.* Therefore, the computer is not fooled by a user's false extension.

[73] COMPUTER AND INFORMATION SECURITY HANDBOOK 307 (John R. Vacca ed., 2009).

[74] *Id.* Professor Kerr breaks this process into two parts: (1) data acquisition, which includes both collecting and preserving the data to be searched; and (2) data reduction, locating the evidence. Kerr, *supra* note 55, at 547. The DOJ Manual describes a two-stage process where first the storage device is imaged and second the device is analyzed for responsive evidence. DOJ MANUAL, *supra* note 54, at 86.

[75] Kerr, *supra* note 55, at 547; *CDT Panel*, 513 F.3d 1085, 1092 (9th Cir. 2008).

[76] Kerr, *supra* note 55, at 540–41.

[77] DOJ MANUAL, *supra* note 54, at 76.

warrant affidavit describe the necessity of removing the entire storage device and imaging it for later examination in a controlled setting.[78] The government contends that the sheer volume of data makes an on-site search too time consuming and invasive.[79] As a result, within the data acquisition phase, the government routinely seeks and receives permission to seize vast amounts of data.[80]

Following the removal of the electronic storage device, investigators preserve the data. The DOJ Manual directs law enforcement to "image" a device before searching it.[81] Imaging creates a bitstream copy of the hard drive by duplicating "every bit and byte on the target drive including all files, the slack space, Master File Table, and metadata in exactly the order they appear on the original."[82] It is essential for the imaging process to preserve the original data without altering any of it.[83] The search is then conducted with forensic software on this bitstream and read-only copy.[84]

After acquiring and preserving the data, investigators search through the information for evidence. Case law describes two broad categories of digital evidence searches. The simplest way to search a computer is to conduct a file-by-file search using the computer's operating system.[85] This type of search involves turning on the computer and manually opening files, for example, files within the My Documents folder or on the desktop.[86] Although simple, this search presents problems because it is time-consuming, inefficient, incomplete, and even destructive.[87] In particular, a file-by-file search requires each file to be opened and examined manually, but will not expose files the user has attempted to conceal or has deleted. More importantly, this type of search alters the metadata of a file, changing the time-date stamp indicating when the file was last accessed.[88] Additionally, a manual search through the computer's

---

[78] *Id.*

[79] *Id.* at 77.

[80] *Id.* at 77–78 (collecting cases allowing off-premises search of entire computers or systems).

[81] *Id.* at 86; *see also* LANGE & NIMSGER, *supra* note 51, at 211–12.

[82] Kerr, *supra* note 55, at 541. When data does not take up the entire cluster, the space between the mark of the end of the file and the end of the cluster is called the "slack space." LANGE & NIMSGER, *supra* note 51, at 236.

[83] *See* LANGE & NIMSGER, *supra* note 51, at 210.

[84] *Id.* at 211–12.

[85] McLain, *supra* note 59, at 1092.

[86] *Id.*; *see, e.g.*, United States v. Walser, 275 F.3d 981 (10th Cir. 2001). In this case, during the search of a suspect's home for evidence of drug use, the agent opened approximately ten files in the "My Documents" folder and then seized the computer to continue the search, opening files in the Recycle Bin and the Program Files folder. *Id.* at 984.

[87] Angeli et al., *supra* note 51, at 19 (citing Jekot, *supra* note 65, at *9); *see also* LANGE & NIMSGER, *supra* note 51, at 212.

[88] COMPUTER AND INFORMATION SECURITY HANDBOOK, *supra* note 73, at 321 & tbl.19.2 (showing examples of date created and modified time stamps recovered with EnCase).

operating system may destroy evidence. Simply using an operating system creates temporary files and risks overwriting reassigned clusters.[89]

Alternatively, a search conducted with forensic software avoids destroying and altering data, while enhancing the investigator's ability to search for evidence.[90] Forensic software bypasses the computer's operating system, thereby increasing the amount of data investigators can access, by not limiting the search to active files.[91] The case *United States v. Mann*[92] illustrates a search conducted with "Forensic Tool Kit" software.[93] In *Mann*, the warrant obtained by the government authorized a search of the defendant's digital and electronic media for images or videos of women in locker rooms or other private areas.[94] After seizing several computers and external hard drives, the investigator first used a write blocker to protect the hard drives from being altered and then created a bitstream copy of each hard drive.[95] Next, Forensic Tool Kit catalogued the images and provided the agent with an overview screen showing how many images, videos, and documents were on the computer, separating them from software files.[96]

Eliminating the irrelevant files, or what some refer to as "data reduction,"[97] is an important function of forensic software. As evident from the search in *Mann*, the crime at issue and the type of evidence the investigators are searching for determines how the data is analyzed. In many cases, the evidence of a crime may not take the form of a file. For example, to prove intent in a child pornography possession case, images of child pornography categorically organized into folders may provide evidence of intentional as opposed to accidental downloading.[98] Similarly, operating system data showing the times users were logged on could help determine the time and sequence of events in a particular crime.[99]

IV. INDIVIDUALS' FOURTH AMENDMENT RIGHTS

The computer search process presents multiple challenges to the Fourth Amendment rights of individuals. First, the broad removal and

[89] LANGE & NIMSGER, *supra* note 51, at 212; *see also* Jekot, *supra* note 65, at *9 (noting that approximately five hundred files are altered during the start-up process of a Windows operating system).

[90] Angeli et al., *supra* note 51, at 19–20 (citing McLain, *supra* note 59, at 1095).

[91] *Id.* (citing McLain, *supra* note 59, at 1095).

[92] 592 F.3d 779 (7th Cir. 2010).

[93] Other forensic software includes Safeback, Snapback, and Linux "dd." LANGE & NIMSGER, *supra* note 51, at 213.

[94] *Mann*, 592 F.3d at 780–81.

[95] *Id.* at 781.

[96] *Id.*

[97] Kerr, *supra* note 55, at 547.

[98] *See* Jekot, *supra* note 65, at *18.

[99] *Id.*; *see also* DOJ MANUAL, *supra* note 54, at 62–63.

imaging of the data allows law enforcement to "seize the haystack to look for the needle,"[100] sanctioning the confiscation of a large amount of data outside the scope of the warrant.[101] Thus, "the normal sequence of 'search' and then selective 'seizure' is turned on its head."[102] Second, a computer search conducted off-site is less time-pressured than physical, on-site searches (such as of a home or a particular room) and analysts can take months to comb through evidence on a computer.[103] Third, courts have historically placed very few limits on what data the investigators can search after making a blanket seizure.[104] Fourth, as *CDT* illustrates, the private data of individuals not suspected of any wrong-doing can easily be swept up, then thoroughly searched. This combination means every electronic data search risks devolving into the very general searches the Framers intended to prohibit.

The Framers crafted the Fourth Amendment to protect citizens against the feared and loathed general warrants, which allowed sweeping, exploratory searches of homes for evidence of seditious libel, and the seizure of anything found.[105] The Fourth Amendment protects an individual from unreasonable searches or seizures of anything in which she has a reasonable expectation of privacy.[106] To have a reasonable expectation of privacy, the person must exhibit an actual expectation of privacy, and it must be recognized by society as reasonable.[107]

The Fourth Amendment specifically mentions the issuance of warrants.[108] To obtain a search warrant, the government must show probable cause and must "particularly describ[e] the place to be searched, and the persons or things to be seized."[109] In a computer search

[100] United States v. Hill, 459 F.3d 966, 975 (9th Cir. 2006).

[101] C*DT En Banc*, 579 F.3d 989, 995 (9th Cir. 2009).

[102] *In re* 3817 W. West End, 321 F. Supp. 2d 953, 958 (N.D. Ill. 2004).

[103] Kerr, *supra* note 55, at 569.

[104] *See, e.g.*, United States v. Gray, 78 F. Supp. 2d 524 (E.D. Va. 1999). In this case, the court held that an agent with a warrant to search a suspect's computer for hacking material (source code) could lawfully examine all the files on the computer—including image files which were clearly not hacking materials. *Id.* at 528–29.

[105] NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 31 (1937). With a writ of assistance, a specialized form of a general warrant, officers of the Crown could "search any house, shop, warehouse, etc.; break open doors, chests, packages . . . and remove any prohibited or uncustomed goods or merchandise." *Id.* at 53.

[106] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[107] *Id.*; California v. Greenwood, 486 U.S. 35, 39–40 (1988) ("An expectation of privacy does not give rise to Fourth Amendment protection, however, unless society is prepared to accept that expectation as objectively reasonable."). This Note assumes that individuals have a reasonable expectation of privacy in the electronic data being searched.

[108] 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 persons or things to be seized.").

[109] *Id.*

context, the government must first demonstrate probable cause that the computer or electronic media is contraband or the fruit of a crime, contains contraband or evidence of a crime, or is an instrumentality of a crime.[110]

A. The Particularity Requirement

The Fourth Amendment also contains the "particularity requirement," which compels a warrant to "particularly describ[e] the place to be searched, and the persons or things to be seized."[111] It further requires the search to be "carefully tailored to its justifications, and . . . not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit."[112] In the physical context, the requirement restricts the places law enforcement may search and what they may seize.[113] To illustrate, an officer with probable cause to search a bedroom for a shotgun would not be able to search the jewelry box on the dresser. A sufficiently particular warrant enables the investigators conducting the search to identify "with reasonable certainty those items that the [issuing] magistrate has authorized him to seize"[114] with a level of specificity that leaves nothing to their discretion.[115] The degree of particularity that is required in any given situation "varies depending on the circumstances of the case and the types of items involved."[116] Defining the level of particularity necessary within electronic searches has proven especially difficult for courts.

The exact contours of the particularity requirement within the electronic data context remain uncertain. For example, the Tenth Circuit ruled a warrant permitting a search of all computer records without a description or limitation may not satisfy the particularity requirement.[117] In contrast, a district court in Massachusetts found a warrant authorizing a search of a "computer and all of its related disks, software and storage devices" to be "sufficiently particular."[118] Further

[110] FED. R. CRIM. P. 41(c).

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

[112] Maryland v. Garrison, 480 U.S. 79, 84 (1987).

[113] *Id.*

[114] United States v. George, 975 F.2d 72, 75 (2d Cir. 1992).

[115] Marron v. United States, 275 U.S. 192, 196 (1927).

[116] *In re* 3817 W. West End, 321 F. Supp. 2d 953, 958 (N.D. Ill. 2004) (quoting United States v. Spilotro, 800 F.2d 959, 963 (9th Cir.1986)).

[117] United States v. Otero, 563 F.3d 1127, 1132–33 (10th Cir. 2009) (holding it overbroad to authorize seizure of any and all information on computer with no limiting instruction); United States v. Riccardi, 405 F.3d 852, 862–63 (10th Cir. 2005) (finding a warrant authorizing the seizure of the computer and all electronic media overbroad).

[118] United States v. Albert, 195 F. Supp. 2d 267, 275–76 (D. Mass. 2002) (holding that warrant authorizing search of a "computer and all of its related disks, software and storage devices was sufficiently particular and narrow"). *See also* People v. Ulloa, 124 Cal. Rptr. 2d 799, 802–05 (Cal. Ct. App. 2002) (holding that warrant authorizing search of

confusing the issue, a district court in Northern Illinois held the particularity requirement necessitates the inclusion of a search methodology in the warrant application.[119] This inconsistency illustrates how the requirement's application within the electronic data context fails to protect individuals against general searches.[120] Interestingly, the *CDT* guidelines set forth new protections for individuals and limits on law enforcement without once mentioning the particularity requirement.

B. The Reasonableness Touchstone and Analogies

When evaluating any search, the court asks "in light of the limitations in the warrant, [was] the execution of the search . . . reasonable[?]"[121] The "general touchstone of reasonableness" governs Fourth Amendment analysis and the "method of execution of the warrant."[122] Within the computer search context, the court's evaluation of the reasonableness of the search often depends upon how the court views computers. Because of the complexity involved, courts frequently analogize electronic data storage devices to physical objects already a part of Fourth Amendment jurisprudence.[123] However, the analogies vary between courts and commentators. To illustrate, some courts view a computer simply as a container.[124] In these cases, the zone of the search encompasses the entire hard drive or storage device.[125] In contrast, in an influential law review article, attorney Raphael Winick argued that, although the container model works for electronic devices with small storage capacities, "the analogy becomes strained when applied to computers with larger storage capacities. For such systems, an analogy to a massive file cabinet, or even to an entire archive or record center, may be more appropriate."[126] Other courts warn comparisons to closed containers or file cabinets "oversimplify a complex area of Fourth Amendment doctrines and ignore the realities of massive modern

"computers [etc.] containing any of the items noted above," which included photographs, videotapes, or movies of simulated or actual sexual acts, was not overbroad).

[119] *In re* 3817 W. West End, 321 F. Supp. 2d at 959, 961.

[120] *See* Kerr, *supra* note 55, at 565, 568.

[121] United States v. Mann, 592 F.3d 779, 782 (7th Cir. 2010).

[122] United States v. Ramirez, 523 U.S. 65, 71 (1998).

[123] McLain, *supra* note 59, at 1072.

[124] United States v. Runyan, 275 F.3d 449, 464–65 (5th Cir. 2001) (comparing ZIP disks to closed containers); People v. Gall, 30 P.3d 145, 153 (Colo. 2001) (finding that "computers found in the defendant's closet were likely to serve as 'containers' for writings" and thus were appropriate to seize when searching for instructions concerning the production or use of any firearms, ammunition, and explosive or incendiary devices or parts). Analogies also vary among commentators. *See* Clancy, *supra* note 13, at 197–200.

[125] Marc Palumbo, Note, *How Safe is Your Data? Conceptualizing Hard Drives Under the Fourth Amendment*, 36 FORDHAM URB. L.J. 977, 978 (2009).

[126] Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 82 (1994).

computer storage."[127] The file cabinet and container analogies also fail to account for the qualitative difference in computer storage.[128] Namely, a computer does not just hold information or files; it is composed of data which it also processes, sorts, and transfers.[129]

The analogies employed by courts impact their analysis of the search's reasonableness. In *United States v. Carey*, the Tenth Circuit discussed the inadequacy of the file cabinet analogy, and ruled that the officer's search of image files was unreasonable because the warrant only authorized a search for names, addresses, and receipts of drug transactions.[130] In doing so, the court determined this case was not comparable to a situation where officers have to open each file cabinet drawer to determine its contents.[131] Alternatively, in *United States v. Runyan*,[132] the Fifth Circuit analogized disks to closed containers. Because the disks had already been compromised by a private search, the court ruled law enforcement's examination of more files within the closed container was reasonable.[133] The disagreement on how to analogize computers produces variations in Fourth Amendment protections. Notably, the *CDT* en banc and per curiam opinions entirely avoided analogizing computers to physical objects.

C. A Special Approach for Computers

The qualitative difference between computers and physical objects has led some courts and commentators to advocate a "special approach" for computer searches. This concept originated with the 1982 Ninth Circuit case *United States v. Tamura*, which concerned the seizure of intermingled paper records.[134] In *Tamura*, during an investigation of an alleged bribery scheme, the FBI executed a warrant authorizing the seizure of corporate documents relating to the scheme.[135] Employees on-site refused to assist the agents in locating the relevant documents and, realizing how long and arduous the search would be without assistance, agents seized several boxes and dozens of file drawers filled with intermingled and unrelated documents.[136] The agents later sifted

[127] United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999) (quoting Winick, *supra* note 126, at 110). *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.").

[128] Gall, 30 P.3d at 162–65 (Martinez, J., dissenting).

[129] Jekot, *supra* note 65, at *18, *27.

[130] *Carey*, 172 F.3d at 1272–73, 1275.

[131] *Id.* at 1275.

[132] 275 F.3d 449 (5th Cir. 2001).

[133] *Id.* at 465; *see also* Clancy, *supra* note 13, at 196 (concluding "computers are containers").

[134] 694 F.2d 591, 595 (9th Cir. 1982).

[135] *Id.* at 594–95.

[136] *Id.* at 595.

through the documents off-site.[137] The court, troubled by the "wholesale seizure for later detailed examination of records not described in a warrant," called the practice the "kind of investigatory dragnet the [F]ourth [A]mendment was designed to prevent."[138] Although the Ninth Circuit did not suppress any of the properly seized documents, the court did establish new safeguards for the wholesale removal of intermingled documents. Specifically, the court instructed that when documents are so intermingled they cannot "feasibly be sorted on site," officers should "seal[] and hold[] the documents pending approval by a magistrate of a further search."[139] If officers know beforehand of the need for "large-scale removal of material," they should seek advance authorization.[140] Thus, any wholesale removal of documents should be monitored by a neutral, detached magistrate to ensure not only that the judge is aware of what she is authorizing, but also that the agents understand the boundaries of the search.[141]

Building upon these safeguards, Winick's article urged courts to apply the *Tamura* rule to computers.[142] He argued that, like the files in *Tamura*, computers also contain innocent and irrelevant material co-mingled with any evidence of criminal activity.[143] Based upon the existence of co-mingled files and the invasiveness of computer searches, he suggested search protocols should be required.[144] Five years later in *Carey*, the Tenth Circuit suggested combining the *Tamura* and Winick approaches to help avoid discovering evidence outside the scope of the warrant in a computer search.[145] The special approach requires officers coming across documents so intermingled as to require off-site sorting to seal and hold the documents pending magistrate approval of conditions and limitations on a further search of the documents.[146]

Those advocating for courts to take a special approach argue that attempting to fit computer searches into physical search frameworks fails to adequately protect individuals from a general search of digital storage devices.[147]

---

[137] *Id.*

[138] *Id.* (quoting United States v. Abrams, 615 F.2d 541, 543 (1st Cir. 1980)).

[139] *Id.* at 595–96.

[140] *Id.* at 596.

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

[142] Winick, *supra* note 126, at 105.

[143] *Id.* at 107.

[144] *Id.* at 107–08.

[145] United States v. Carey, 172 F.3d 1268, 1275 n.8 (10th Cir. 1999).

[146] *Id.* at 1275. A year later, the Tenth Circuit reemphasized this point—that the additional step of sorting the documents may be required when computers contain intermingled documents. United States v. Campos, 221 F.3d 1143, 1148 (10th Cir. 2000).

[147] McLain, *supra* note 59, at 1077; Derek Haynes, Comment, *Search Protocols: Establishing the Protections Mandated by the Fourth Amendment Against Unreasonable Searches and Seizures in the World of Electronic Evidence*, 40 MCGEORGE L. REV. 757, 762 (2009).

V. THE *CDT* GUIDELINES

Against this backdrop of awkward analogies and unpredictable applications of the particularity requirement, the Ninth Circuit decided *CDT*. Going beyond what was needed to resolve the case, in Judge Kozinski's en banc opinion, the court originally introduced the guidelines by declaring "[e]veryone's interests are best served if there are clear rules to follow that 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."[148] Accordingly, to prevent the process of segregating electronic data from becoming a means for government to access data it has no probable cause to collect, the court proposed the following five guidelines: (1) magistrates should insist that the government waive reliance upon the plain view doctrine in digital evidence cases; (2) specialized personnel or independent third parties should segregate and redact the data; (3) warrants and subpoenas must disclose the actual risks of destruction of evidence; (4) the government must design a search protocol to uncover only the information for which probable cause exists; and (5) the government must destroy or return non-responsive data.[149]

The dissent criticized the opinion for granting heightened Fourth Amendment protections to computer searches without citing to legal authority to support the new rules.[150] With this criticism in mind, this Part critically examines four of the five guidelines, attempting to find caselaw to support them. The discussion of the fifth guideline concerning the Rule 41(g) return of property falls beyond the scope of this Note.

A. Forswearing Plain View

1. Reaction to the Plain View Argument

The first guideline proposed in *CDT* indicates its importance both to the facts of the case and to the court's attempt to prevent computer searches from becoming prohibited general searches. In this case, the government conceded it lacked probable cause to search or seize any data beyond the ten players listed within the warrant.[151] Instead, the government justified the warrantless seizure of the unnamed players' testing results by claiming the data came into plain view while agents examined the Tracey Directory.[152] Many of the judges involved in this case, at both the district and appellate level, expressed grave concerns over the staggering implications of the application of the plain view

[148] *CDT En Banc*, 579 F.3d 989, 1006 (9th Cir. 2009).

[149] *Id.*

[150] *Id.* at 1012–13 (Callahan, J. concurring in part and dissenting in part).

[151] *CDT Panel*, 513 F.3d 1085, 1147 (9th Cir. 2008) (Thomas, J., concurring in part and dissenting in part).

[152] *CDT En Banc*, 579 F.3d at 997.

doctrine within the electronic data context.[153] Although the majority in the panel decision did not reach the plain view question,[154] Judge Thomas in a lengthy dissent concluded that the plain view doctrine clearly has no application to intermingled private electronic data.[155] Further, in both the en banc and per curiam opinions, the court determined the doctrine's application produced "illogical results" and created a great risk for abuse.[156]

Prior to *CDT*, other courts and commentators also expressed unease applying the plain view doctrine to the computer search context. For example, the Tenth Circuit in *Carey,* although declining to determine what constitutes plain view in "the context of computer files," explicitly rejected the government's argument that closed image files were in plain view.[157] Additionally, Professor Orin Kerr, who has written extensively on searches within the digital context and helped author the DOJ computer search manual,[158] recognized that eventually "abolishing the plain view exception [within the digital context] may best balance the competing needs of privacy and law enforcement."[159]

2. The Plain View Doctrine

The plain view doctrine operates as an exception to the Fourth Amendment's warrant requirement, allowing law enforcement to seize evidence outside the scope of the warrant, or without a warrant at all, so long as the following four conditions are met. First, the officer must be lawfully in a position from which he views the object. Thus, the initial intrusion bringing the officer into plain view of the object must be

[153] *CDT Panel*, 513 F.3d at 1117, 1124–25 (Thomas, J. concurring in part and dissenting in part) (noting his concerns and those of the district judges).

[154] *Id.* at 1112 n.48.

[155] *Id.* at 1117 (Thomas, J., concurring in part and dissenting in part).

[156] *See CDT En Banc*, 579 F.3d at 998; *CDT Per Curiam*, 621 F.3d 1162, 1170–71 (9th Cir. 2010).

[157] United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999). Notably, the court confused the issue of the plain view doctrine within the computer context by considering the officer's subjective intent. Specifically, the court emphasized that the officer's discovery of the child pornography files was not inadvertent because the officer abandoned his search for evidence of drug trafficking to look for more evidence of child pornography. *Id.* Importantly, within the plain view context, the Supreme Court has ruled that although "inadvertence is a characteristic of most legitimate 'plain-view' seizures, it is not a necessary condition." Horton v. California, 496 U.S. 128, 130 (1990).

[158] *See, e.g.*, Kerr, *supra* note 55; Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004); DOJ MANUAL, *supra* note 54, at vii. Professor Kerr has also been cited by courts addressing search and seizure issues within the digital context. *See, e.g.*, United States v. Vilar, No. S305CR621KMK, 2007 WL 1075041, at *35 & n.22 (S.D.N.Y. Apr. 4, 2007).

[159] Kerr, *supra* note 55, at 583; *see also* RayMing Chang, *Why the Plain View Doctrine Should Not Apply to Digital Evidence*, 12 SUFFOLK J. TRIAL & APP. ADVOC. 31, 36–37 (2007) (positing that although drastic, eliminating the plain view exception in computer contexts would best protect against general searches).

justified and not itself a violation of the Fourth Amendment.[160] When an officer is lawfully in a position where he views the object in plain view, neither the observation nor its seizure involves a further invasion of privacy.[161] Second, the object must be in plain view. The original application of this doctrine contemplated situations where physical evidence or objects seized were "obvious to the senses."[162] Third, the incriminating nature of the object must be immediately apparent.[163] When an officer must conduct a further search of an object to determine if there is probable cause that the object is indeed contraband or evidence, it is not in plain view.[164] Finally, the officer must have a lawful right of access to the object itself.[165] Even assuming all of these requirements are met, the Supreme Court instructs that the plain view doctrine "may not be used to extend a general exploratory search from one object to another until something incriminating . . . emerges."[166]

The Supreme Court unequivocally stated that "plain view *alone* is never enough to justify the warrantless seizure of evidence."[167] In the majority of cases, any evidence seized will be in plain view at the moment of seizure. As a result, the court must "identify the circumstances in which plain view has legal significance rather than being simply the normal concomitant of any search, legal or illegal."[168]

3. Support for Forswearing the Plain View Doctrine

Application of the plain view doctrine within the computer search context both belies the practical justifications for the doctrine and proves unworkable within this context.[169]

a. Undermining the Original Justification

The plain view doctrine seeks to spare police "the inconvenience and the risk—to themselves or to preservation of the evidence—of going to obtain a warrant."[170] However, this justification is inapplicable during a search of electronic data in a controlled environment for at least three reasons. First, in such a controlled environment, no danger to the officer

[160] *Horton*, 496 U.S. at 135–36 (1990).

[161] *Id.*

[162] United States v. Sifuentes, 504 F.2d 845, 848 (4th Cir. 1974); Minnesota v. Dickerson, 508 U.S. 366, 375–76 (1993) (describing how tactile discoveries of contraband, such as drugs discovered when lawfully patting down a suspect, are "justified by the same practical considerations that inhere in the plain-view context").

[163] Coolidge v. New Hampshire, 403 U.S. 443, 466 (1971).

[164] *Dickerson*, 508 U.S. at 375.

[165] *Id.*

[166] *Coolidge*, 403 U.S. at 466.

[167] *Id.* at 468.

[168] *Id.* at 465.

[169] Angeli et al., *supra* note 51, at 23.

[170] Arizona v. Hicks, 480 U.S. 321, 326–27 (1987). *See also Coolidge*, 403 U.S. at 468 (noting similar reasons for the plain view doctrine).

exists.[171] Second, the digital evidence is not at risk.[172] Specifically, each forensic search of a computer begins with law enforcement making a bitstream copy of the storage device.[173] Third, a search in this environment affords the government both the time and opportunity to seek additional warrants when necessary.[174] Indeed, the government takes the position that the Fourth Amendment puts no time limit restrictions upon computer forensic searches.[175] Consequently, off-site examination of computer data upsets the "basic assumptions underlying the plain view doctrine."[176]

Most importantly, it is unclear what the justification is for applying the plain view doctrine to the digital context. In its brief asking for a full en banc rehearing, the government failed to explain why the plain view doctrine should apply to computer contexts, ignoring the court's concern that the application of plain view to computer contexts allows de facto general searches.[177] Perhaps in the context of digital evidence, if the government prefers not to forswear plain view, the government should bear the burden to establish why the doctrine applies to computer searches.[178]

b. Unclear Function Within the Digital Storage Context

The plain view doctrine is unworkable within the computer context because courts disagree on how to apply Fourth Amendment concepts in light of the nature and scope of computer data. Some courts have determined computer searches warrant a "special approach" granting heightened Fourth Amendment protections,[179] whereas other courts explicitly reject such an approach. For example, the Ninth Circuit in

[171] Angeli et al., *supra* note 51, at 23.

[172] *Id.*

[173] DOJ MANUAL, *supra* note 54, at 86.

[174] *CDT Panel*, 513 F.3d 1085, 1146 (9th Cir. 2008) (Thomas, J., concurring in part and dissenting in part).

[175] DOJ MANUAL, *supra* note 54, at 91–95. Additionally, courts have upheld forensic analyses begun months after investigators acquire a computer or data. *See* United States v. Burns, No. 07 CR 556, 2008 WL 4542990, at *8–9 (N.D. Ill. Apr. 29, 2008) (upholding a ten-month delay); United States v. Gorrell, 360 F. Supp. 2d 48, 55 n.5 (D.D.C. 2004) (upholding a ten-month delay); United States v. Hernandez, 183 F. Supp. 2d 468, 480 (D.P.R. 2002) (upholding a six week delay).

[176] Kerr, *supra* note 55, at 576–77; *see CDT Panel*, 513 F.3d at 1146 (Thomas, J., concurring in part and dissenting in part).

[177] CDT Appellant Brief, *supra* note 6, at 8–9; *CDT En Banc*, 579 F.3d 989, 1005 (9th Cir. 2009) (stating concern that "[a]uthorization to search *some* computer files therefore automatically becomes authorization to search all files").

[178] *See CDT Panel*, 513 F.3d at 1124 (Thomas, J., concurring in part and dissenting in part) (describing District Judge Illston's finding that the government failed to provide any case to "support its contention that the plain view doctrine applied in the computer context").

[179] *See, e.g.*, United States v. Carey, 172 F.3d 1268, 1275 nn.7–8 (10th Cir. 1999) (quoting Winick, *supra* note 126, at 108); United States v. Campos, 221 F.3d 1143, 1148 (10th Cir. 2000).

2008 rejected taking a special approach based upon specific technologies, concluding officers can search a computer just as they may search a room full of filing cabinets.[180] Even those courts agreeing that a special approach is not required by the Fourth Amendment disagree on how to adapt physical-world search concepts to digital evidence, employing various, conflicting analogies.[181]

Such differing views make it impossible to determine the threshold question of whether or not an officer is lawfully in a place where the object came into plain view. Namely, if the container analogy applies—what exactly is the container? Some courts identify the computer itself as the container, potentially placing every file or even cluster of data into plain view. Judge Bea's concurrence and dissent in the *CDT* en banc opinion represents the other extreme. Specifically, Judge Bea reasoned that to put the results of the unnamed players validly within plain view, the agent must have displayed only the testing results for the players named in the warrant and could only have seized "evidence of additional illegality if such evidence is 'immediately apparent' as part of the *segregated* results for those ballplayers."[182] These opposing views are difficult (if not impossible) to reconcile and demonstrate that, depending upon the court's view, electronic data may either always or never be in plain view.

c. Electronic Data May Either Always or Never Be in Plain View

i. Always in Plain View

The over-seizing of electronic data combined with the permission to search every file on a computer means law enforcement may always be in a position where everything in a computer is in plain view.[183] The Ninth Circuit acknowledged that the over-seizing of electronic data is "an inherent part of the electronic search process."[184] Importantly, the government determines how much data to seize. Once data is seized, many courts allow the government to examine each and every file to determine if it falls within the scope of the warrant.[185] As a result, everything in the computer could be in plain view.

---

[180] United States v. Giberson, 527 F.3d 882, 888 (9th Cir. 2008).

[181] *See infra* Part IV.C.

[182] *CDT En Banc*, 579 F.3d 989, 1016 (9th Cir. 2009) (Bea, J., concurring in part and dissenting in part); *CDT Per Curiam*, 621 F.3d 1162, 1181 (9th Cir. 2010).

[183] *See* Chang, *supra* note 159, at 36–37 (posing questions as to the extent of plain view in the digital context).

[184] *CDT En Banc*, 579 F.3d at 1006; *CDT Per Curiam*, 621 F.3d at 1177.

[185] *CDT Per Curiam*, 621 F.3d at 1170–71 (stating "we have no cavil with [the] general proposition" that the government can carefully examine the contents of every file); United States v. Fumo, 565 F. Supp. 2d 638, 649 (E.D. Pa. 2008) ("[T]he nature of computer files [allows] the government [to] legally open and briefly examine each file when searching a computer pursuant to a valid warrant."); United States v. Gray, 78 F. Supp. 2d 524, 528 (E.D. Va. 1999).

However, the proposition that everything is within plain view conflicts with the Supreme Court's instruction that the doctrine may not be used to transform a valid search into a prohibited general search.[186] Additionally problematic, this position bestows a great advantage upon law enforcement at great cost to an individual's Fourth Amendment rights.

ii. Never in Plain View

The nature of electronic data raises the question: is computer data ever in plain view?[187] In its application of the plain view doctrine, the Supreme Court contemplated situations in which the evidence in question was "obvious to the senses."[188] However, electronic data is a collection of ones and zeros requiring special devices to translate it into something meaningful.[189] Thus, within the computer search context, the evidence is

> not in plain view in the sense of walking into the room and seeing the scale on the desk. It takes a whole lot of work to get there. . . . [T]here are whole industries that have developed in order to make it possible for the disk to show up on the screen that way.[190]

Significantly, any minor disturbance of an object to place it in plain view is fatal to the application of the doctrine. For example, in *Arizona v. Hicks*, officers searching an apartment for weapons noticed expensive stereo equipment that looked out of place in the squalid apartment.[191] One officer moved some of the components to read and record their serial numbers, later determining them to be stolen.[192] The Supreme Court found this minor disturbance a violation of the plain view doctrine.[193] The Court ruled that exposing concealed portions of the apartment or its contents while taking any action unrelated to the objectives of the authorized intrusion produces a new invasion of privacy.[194] Therefore, any interference with the computer system by the government, as obvious as decrypting encrypted files,[195] or as subtle as scrolling down through an open document to view the data not displayed

---

[186] *See* Horton v. California, 496 U.S. 128, 137–38 (1990).

[187] Angeli et al., *supra* note 51, at 23.

[188] United States v. Sifuentes, 504 F.2d 845, 848 (4th Cir. 1974); s*ee, e.g.*, Minnesota v. Dickerson, 508 U.S. 366, 375–76 (1993).

[189] McLain, *supra* note 59, at 1091; *see also CDT Panel*, 513 F.3d 1085, 1146 (9th Cir. 2008) (Thomas, J., concurring in part and dissenting in part).

[190] *CDT Panel*, 513 F.3d at 1124 (Thomas, J., concurring in part and dissenting in part) (quoting District Judge Illston).

[191] 480 U.S. 321, 323 (1987).

[192] *Id.*

[193] *Id.* at 324–25.

[194] *Id.* at 325.

[195] United States v. Kim, 677 F. Supp. 2d 930, 943, 948, 950 (S.D. Tex. 2009) (holding materials within an encrypted file are not immediately visible to law enforcement).

on the screen,[196] interferes with the computer system and exposes concealed portions, thereby producing a new invasion of privacy and violating the plain view doctrine.[197]

d. Preventing General Searches

Finally, waiving reliance on the plain view doctrine may be the best way to prevent computer searches from becoming de facto general searches. In particular, granting law enforcement the authority to open any and every file within a computer allows a vast amount of data to arguably come within plain view. As both the en banc and per curiam opinions emphasized, since government agents decide how much data to actually take, this creates a powerful incentive to seize more rather than less.[198] At the same time, limits that apply to traditional physical evidence searches do not apply in computer searches.[199] For example, unlike in traditional physical searches, the particularity requirement does nothing to guard against seeking a warrant for a low-level crime as a pretext to conduct a general, exploratory search for evidence of any crime.[200] Indeed, in *CDT*, the agent admitted that the idea behind taking the Tracey Directory was to "briefly peruse it to see if there was anything above and beyond that which was authorized for seizure in the initial warrant."[201] Ultimately, applying the plain view doctrine in the computer search context violates the Supreme Court's instruction in *Coolidge*, that the "doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges."[202] As a result, support exists for the first guideline proposed in *CDT*.

B. Segregation Teams

The second guideline in *CDT* recommends the use of specialized personnel or an independent third party to complete the segregation

[196] *CDT En Banc*, 579 F.3d 989, 1016 (9th Cir. 2009) (Bea, J., concurring in part and dissenting in part).

[197] *See* Donald Resseguie, Note, *Computer Searches and Seizure*, 48 CLEV. ST. L. REV. 185, 191 (2000).

[198] *CDT En Banc*, 579 F.3d at 998–99. In fact, Judge Kozinski concluded "[t]he government agents obviously were counting on the search to bring constitutionally protected data into the plain view of the investigating agents." *Id. See also CDT Per Curiam*, 621 F.3d 1162, 1171 (9th Cir. 2010).

[199] Kerr, *supra* note 55, at 569.

[200] Chang, *supra* note 159, at 46. Chang describes a situation where police target an individual for illegal possession of copyrighted material, a crime nearly everyone with a computer is at risk of committing and which would be easy to establish probable cause for. Once police have the computer, everything on the storage device could be examined and used against the individual.

[201] *CDT En Banc*, 579 F.3d at 999 (internal quotation marks omitted).

[202] Coolidge v. New Hampshire, 403 U.S. 443, 466 (1971).

and redaction of data.[203] Depending upon the "nature and sensitivity of the privacy interests involved," the magistrate may also appoint an independent expert or special master to conduct or supervise the segregation.[204] Specifically, when the investigation involves third parties not under any criminal suspicion, the segregation must be conducted by or at least closely supervised by an independent third party.[205] Following the segregation process, personnel may not share the information learned during this process with the case agent, "absent further approval of the court."[206]

Notably, this guideline originated within the government's own warrant application. In particular, after putting forth a case for a broad seizure of data, the government represented that "computer personnel" would conduct the initial review, segregating the materials and returning those not subject to the warrant.[207] Despite this representation, the case agent assumed control over the entire Tracey Directory and its thousands of files, viewing all of the data, before any segregation occurred.[208] The court not only ruled this procedure violated the protocol set forth in the warrant, but decided to impose a similar requirement upon future computer searches.[209]

1. Segregation Teams

The use of a segregation team is not a novel concept. When searching the records of law firms, which contain documents protected by the attorney–client privilege, law enforcement sometimes uses what is referred to as a "privilege" or "taint" team.[210] Taint teams include investigators and prosecutors not involved in the main investigation who conduct the search separately and independently from the case agents

[203] *CDT En Banc*, 579 F.3d at 1000, 1006.

[204] *Id.* at 1000.

[205] *Id.*

[206] *Id.*

[207] *Id.* at 999; *CDT Panel*, 513 F.3d 1085, 1133–34 (9th Cir. 2008) (Thomas, J., concurring in part and dissenting in part) (describing Judge Cooper's finding that the warrant required the seized items not covered by the warrant to be screened and segregated first by computer personnel, requiring more than a mere consultation or participation, and instead requiring "appropriately trained personnel" to first screen and segregate the data not covered by the warrant). It should be noted that the dissent in the en banc opinion and the majority of the panel opinion drew different inferences from the language within the warrant. For example, Judge Callahan believed the warrant did not expressly limit the initial review to computer specialists and exclude other agents. *CDT En Banc*, 579 F.3d at 1011 (Callahan, J., concurring in part and dissenting in part). The government also argued that it did not specify only computer personnel could examine the seized files. *Id.* at 1000.

[208] *CDT En Banc*, 579 F.3d at 999.

[209] *Id.* at 1000.

[210] UNITED STATES ATTORNEYS' MANUAL § 9-13.420(E) (2011), *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/13mcrm.htm; *In re* Grand Jury Subpoenas, 454 F.3d 511, 515 (6th Cir. 2006).

and prosecutors.[211] As a result, the team separates the privileged information, while keeping the case agents and prosecutors from being "tainted" by viewing privileged information they cannot later use within the prosecution.[212] *United States v. Neill* illustrates the use of a taint team.[213] In *Neill*, a warrant authorized the search of an attorney's home and law office.[214] To prevent intrusions into the attorney–client privilege, the government used FBI attorneys to segregate potentially privileged documents into sealed envelopes and boxes.[215] Later, attorneys not involved in the investigation reviewed the materials, while remaining "walled off" from the prosecution team, attempting to ensure that the prosecution team remained free from any "'taint' arising from exposure to potentially privileged material."[216]

Courts examining the use of taint teams have questioned not only their fairness, but also any appearance of unfairness. The protection provided by this team relies heavily upon the strength of the "wall" erected between the examining agents and the case agents.[217] The strength can be impacted by both the government examiner's conflict of interest leading to a violation of ethical obligations and by simple human mistakes.[218] Ultimately, the use of taint teams is not mandated in privilege situations, but is considered an imperfect tool.

2. Support for the Segregation Team Guideline

Judge Kozinski draws support for the guideline requiring the use of a segregation team from *Tamura*.[219] *Tamura* requires a neutral and detached magistrate to monitor the wholesale removal of intermingled documents in order to maintain the privacy of the materials falling outside the scope of the warrant.[220] Previously, the Tenth Circuit also applied *Tamura* to computer searches. In *Carey*, the Tenth Circuit combined the safeguards in *Tamura* with the approach Winick advocated to avoid discovering evidence outside the scope of the warrant in a computer search.[221] In particular the court instructed that whenever

[211] *See id.* at § 9-13.430; *In re Grand Jury Subpoenas*, 454 F.3d at 515.

[212] When privileged documents are involved, a taint team can be used in lieu of submitting contested materials to the magistrate to review in camera. *See, e.g.*, United States v. Neill, 952 F. Supp. 834, 840–41 (D.D.C. 1997).

[213] 952 F. Supp. at 836–37.

[214] *Id.*

[215] *Id.* at 837.

[216] *Id.*

[217] *In re* Grand Jury Subpoenas, 454 F.3d 511, 512 (6th Cir. 2006).

[218] *Id.* at 523; *see also* United States v. Stewart, No. 02 CR 396 JGK, 2002 WL 1300059, at *8 (S.D.N.Y. June 11, 2002) ("It is a great leap of faith to expect that members of the general public would believe that any such Chinese wall would be impenetrable; this notwithstanding the honor of an AUSA." (quoting *In re* Search Warrant for Law Offices Executed on March 19, 1992, 153 F.R.D. 55, 59 (S.D.N.Y. 1994))).

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

[220] *Id.* at 595–96; *CDT En Banc*, 579 F.3d 989, 996 (9th Cir. 2009).

[221] United States v. Carey, 172 F.3d 1268, 1275 & nn.6, 8 (10th Cir. 1999).

officers come across documents so intermingled as to require off-site sorting, the documents should be sealed and held pending magistrate approval of conditions and limitations applied to a further search of the documents.[222] Similarly, in *CDT*, the court ruled that simply accepting the justification for wholesale seizure without any further safeguards or limitations renders *Tamura* useless.[223] Although not joining the majority en banc opinion, Judge Bea stated that *Tamura* requires the magistrate to oversee the search process of intermingled documents, and suggested: "perhaps the instant case counsels that such oversight ought to be quite close."[224]

The use of a segregation team or special master simply supplants the magistrate's role in overseeing the search of intermingled documents. Indeed, *Tamura* contemplates the use of certain individuals to minimize unwarranted intrusions into privacy.[225] Courts have routinely upheld the involvement of citizens serving a legitimate investigative function to facilitate searches. For example, law enforcement often uses lay experts or employees to facilitate on-site searches by helping identify technical documents or specific equipment.[226]

3. Contrary Case Law

Despite previous use of individuals to help segregate data, their use has never been required. In *Andresen v. Maryland,* the Supreme Court accepted the proposition that case agents will examine some innocuous documents "at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized."[227] Some courts extend this to the computer context, reasoning that a brief review of electronic documents in order to determine which ones fall within the scope of the

[222] *Id.* at 1275.

[223] *CDT En Banc*, 579 F.3d at 998. The per curiam opinion keeps all of the en banc's language concerning *Tamura*. *CDT Per Curiam*, 621 F.3d 1162, 1170–71 (9th Cir. 2010).

[224] *CDT En Banc*, 579 F.3d at 1018 (Bea, J., concurring in part and dissenting in part). Interestingly, although Judge Bea's concurrence in the per curiam opinion closely resembles his en banc concurrence, this particular language on magistrate oversight is missing. *See CDT Per Curiam*, 621 F.3d at 1180–83 (Bea, J., concurring in part and dissenting in part). Other judges have also raised *Tamura* concerns. Specifically, in his dissent from the panel opinion, Judge Thomas stated *Tamura* requires a neutral and detached magistrate to review the records before allowing the government to do so. *CDT Panel*, 513 F.3d 1085, 1136 (9th Cir. 2008) (Thomas, J., concurring in part and dissenting in part).

[225] United States v. Tamura, 694 F.2d 591, 596 n.4 (9th Cir. 1982).

[226] *Id.* (citing Forro Precision, Inc. v. IBM Corp., 673 F.2d 1045, 1053–54 (9th Cir. 1982)) (upholding a search where IBM employees accompanied police officers executing a search warrant to help identify technical documents); *see also* Bellville v. Town of Northboro, 375 F.3d 25, 32–33 (1st Cir. 2004) (using company officials for their technical expertise and knowledge of the items belonging to the company in a search of a home office related to an investigation of stolen computer chips and equipment from an electronics company).

[227] 427 U.S. 463, 482 n.11 (1976).

warrant is directly comparable to the paper document context.[228] Similarly, both the en banc and per curiam opinions declare to have "no cavil" with the general proposition that the government must carefully examine the contents of files to determine whether or not relevant data has been concealed.[229]

However, *Andresen* does not foreclose requiring the use of segregation teams. *Andresen* also instructs judicial officials to "take care to assure that [searches] are conducted in a manner that minimizes unwarranted intrusions upon privacy."[230] This instruction helps lay the foundation for the use of segregation teams and the guideline advising law enforcement to establish search protocols.

4. A Compromise Going Forward

With this in mind, courts reluctant to apply an overall special approach to computer searches could narrow the application of the segregation team guideline. Namely, courts could apply this guideline only to the limited context of seizing and searching the confidential information of third parties not suspected of any wrongdoing. The use of a segregation team is particularly valuable and important where the data of third parties, not under criminal suspicion, is at risk. In fact, both Congress and the Attorney General have recognized the concerns raised by executing search warrants in these situations. Specifically, the Attorney General issued guidelines for obtaining documentary materials from disinterested third parties, such as doctors, lawyers, or clergy members not implicated in the subject of the crime under investigation.[231] Moreover, Congress explicitly recognized privacy in medical records, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[232] In his dissent from the panel opinion, Judge Thomas argued that not using a segregation team when medical records are at issue essentially entitles the government not only to seize but also to view

[228] Manno v. Christie, Civ. No. 08-3254 (RBK), 2008 WL 4058016, at *4 (D.N.J. Aug. 22, 2008); United States v. Potts, 559 F. Supp. 2d 1162, 1175–76 (D. Kan. 2008) (warrant did not authorize an overbroad search when it allowed the investigator "to search the computer by . . . 'opening' or cursorily reviewing the first few 'pages' of such files in order to determine the precise content").

[229] *CDT Per Curiam*, 621 F.3d 1162, 1171 (9th Cir. 2010); *CDT En Banc*, 579 F.3d at 998.

[230] *Andresen*, 427 U.S. at 482 n.11. Interestingly, the DOJ Manual points out that this phrase within *Andresen* has been used by magistrates in requiring the government to set forth a search strategy. DOJ MANUAL, *supra* note 54, at 81.

[231] Guidelines on Methods of Obtaining Documentary Materials Held by Third Parties: Procedures, 28 C.F.R. § 59.4 (2010) (requiring federal officials to use subpoenas in lieu of search warrants, unless less intrusive means would "substantially jeopardize the availability or usefulness of the materials sought").

[232] Pub. L. No. 104-191, § 264, 110 Stat. 1936, 2033 (1996); *see also CDT Panel*, 513 F.3d 1085, 1138 (9th Cir. 2008) (Thomas, J., concurring in part and dissenting in part).

the medical records of "anyone who had the misfortune of visiting . . . a health care provider" subject to a search warrant.[233]

Limiting this guideline's application also addresses the practical concerns of requiring the use of segregation teams. For example, this guideline requires law enforcement to keep a computer forensic analyst "walled off" from other officers. This may involve costly personnel expansion for local law enforcement agencies or the use of third party consultants which may prove unworkable and unaffordable for smaller departments.[234] Additionally, in more complicated cases, such as fraud, the computer analysts may have to be trained on the specifics of the case in order to identify responsive data.[235] Because the analysts will have less experience with the nuances of the case, responsive data may even go undetected.[236]

On a larger level, the segregation team guideline applied in a limited context carries some advantages over the other suggested *CDT* guidelines. In particular, segregation teams avoid some of the problems unique to crafting *ex ante* search protocols for a forensic process described as "contingent, fact-bound, and quite unpredictable."[237] Agents may often not know what type of software is on the computer, what types of files are contained on the hard drive, or if the suspect took any steps to conceal, disguise, or delete files.[238] Using a segregation team will not require adapting to new technologies to craft an *ex ante* strategy. It also could prevent confusion stemming from courts trying to adapt old statutory regimes built around outdated technology to new technologies.[239] Similarly, it avoids judicial misunderstandings of technology.[240] Consequently, there is both support and practical justification for this narrow application of the segregation team guideline.

---

[233] *CDT Panel*, 513 F.3d at 1141–42 & n.15 (Thomas, J., concurring in part and dissenting in part).

[234] *CDT En Banc*, 579 F.3d 989, 1013 (9th Cir. 2009) (Callahan, J., concurring in part and dissenting in part); CDT Appellant Brief, *supra* note 6, at 17–18 (arguing that use of independent consultants potentially puts the security of some investigations at risk, particularly those involving confidential informants or classified information).

[235] CDT Appellant Brief, *supra* note 6, at 16.

[236] *Id.*

[237] Kerr, *supra* note 55, at 575.

[238] *Id.*

[239] Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 773 (2005).

[240] United States v. Hill, 459 F.3d 966 (9th Cir. 2006). In this case, the judge believed that in order to properly search computers on-site, law enforcement would need computers equipped with different operating systems in order to search through files. *Id.* at 974.

C. Disclosing the Actual Risks of the Search

Of the four guidelines this Note discusses, the third recommendation to disclose the actual risks of the computer search proves most supportable. This guideline suggests that, in warrants and subpoenas, the government should both disclose the actual risks of destruction of data and the prior efforts to seize the information in other judicial fora.[241] While acknowledging the government may not know the actual risks it will encounter in a search, "omitting such highly relevant information altogether is inconsistent with the government's duty of candor in presenting a warrant application" and "shall bear heavily against the government in the calculus of any subsequent motion to return or suppress the seized data."[242] The wording of this guideline reveals its close tailoring to the facts at issue in *CDT* and the court's specific concerns with the government's conduct. Nevertheless, its underlying theme applies to any search of digital data and reveals some recurring problems with warrants and affidavits in computer searches.

Previously, the Ninth Circuit required the government to explain the reasonableness of a broad search and seizure of electronic data in the affidavit for a search warrant.[243] In *Hill*, a computer repair technician discovered what she believed to be child pornography while repairing the defendant's computer, and alerted the police.[244] The police obtained a warrant authorizing a search of all storage media belonging to the defendant.[245] Hill argued that authorizing the seizure and removal of the computer and storage media without determining whether they contained child pornography was too broad.[246] In its decision, the court compared computer searches to those of the intermingled documents in *Tamura*, concluding that the blanket removal of storage media required a reasonable explanation within the affidavit.[247] Importantly, the court cautioned that without the presentation of this information, there is no way to know if the approving magistrate made an informed decision regarding the merits of a blanket seizure.[248]

An "informed decision," requires the magistrate to consider more than generic hazards. The Fourth Amendment's demand for a factual

---

[241] *CDT En Banc*, 579 F.3d 989, 1006 (9th Cir. 2009). In this case, the government requested subpoenas and warrants in three different districts. Additionally, the day the defense filed a motion to quash a subpoena, the government obtained a search warrant for the same location. *Id.* at 993–94.

[242] *Id.* at 998–99.

[243] *Hill*, 459 F.3d at 976.

[244] *Id.* at 968.

[245] *Id.*

[246] *Id.* at 973. Additionally, Mr. Hill contended the police are required to bring equipment to separate the responsive data from the nonresponsive. However, the court determined such a requirement posed too many technical problems and would take too much time. *Id.* at 974.

[247] *Id* at 976.

[248] *Id.*

showing to establish probable cause assumes there will be a truthful showing in the oath or affirmation supporting the warrant.[249] Even though this does not require every fact included in the warrant to be correct, it must be "'truthful' in the sense that the information put forth is believed or appropriately accepted by the affiant as true."[250]

Up until *CDT*, it appeared that the government's recitation of generic hazards sufficed. Generally, the government takes the position that imaging or removal of an entire electronic storage device is necessary in nearly every computer search case.[251] Courts have routinely agreed.[252] In *CDT*, in order to justify a broad seizure, the government included in the warrant numerous possible ways the data could be destroyed.[253] In particular, the government explained that computer files can be disguised by misleading names and extensions, deleted, encrypted, password-protected, or even "booby-trapped" (where data is destroyed if certain procedures are not "scrupulously followed").[254] Although arguably appropriate in some situations, in *CDT* these theoretical and generic risks failed to address the specifics of the situation. For example, citing only theorized risks ignored the fact that CDT, Inc. agreed to keep all data intact pending the resolution of its motion to quash.[255] The generic language also disregarded the fact that CDT, Inc. is a legitimate business, not suspected of any wrongdoing. Further, the warrant application did not identify why the government determined data would be so ingeniously disguised in this particular circumstance. The court found that the affidavit's absence of individualized justification prevented it from determining if the magistrate "was aware of the officers' intent and the technological limitations meriting the indiscriminate seizure—and thus was intelligently able to exercise the court's oversight function."[256]

Requiring the government to describe only generalized risks in every computer search case leads to illogical results. If it is always unreasonable to require law enforcement to conduct on-site searches of electronic

[249] Franks v. Delaware, 438 U.S. 154, 164–65 (1978).

[250] *Id.* at 165.

[251] DOJ MANUAL, *supra* note 54, at 76, 78.

[252] A sampling of cases on point reveals the generic boilerplate language used to justify broad seizure. *See, e.g.*, United States v. Campos, 221 F.3d 1143, 1147 (10th Cir. 2000) (accepting the government's position that searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment due to the data's vulnerability to tampering and destruction); United States v. Maali, 346 F. Supp. 2d 1226, 1245–46 (M.D. Fla. 2004) (agreeing to a broad seizure based upon an agent's representation that the volume of evidence and the possibility of concealment required the seizure of most or all computer equipment).

[253] *CDT En Banc*, 579 F.3d 989, 998 (9th Cir. 2009).

[254] *Id.* at 995.

[255] *Id.* at 998.

[256] *CDT Panel*, 513 F.3d 1085, 1110 (9th Cir. 2008) (quoting United States v. Hill, 459 F.3d 966, 976 (9th Cir. 2006)).

data, then it is not reasonable, nor necessary, to explain in each affidavit why on-site searches are impractical.[257] If the need for blanket seizure is not fact-specific, it does not change based upon the magistrate's technical knowledge, or lack thereof.[258] Thus, requiring the government to include this language within an affidavit serves no real purpose, unless it is more thoughtfully applied.

Additionally problematic, some generic hazards are based upon debunked myths which may even mislead the court. For example, in *Hill*, the court found it unreasonable to search digital data on-site because "computers in common use run a variety of operating systems."[259] As a result, the court believed in order to search on-site, law enforcement would need to bring computers equipped to read all types of files on all types of operating systems.[260] However, using forensic software, which bypasses operating systems, renders this justification outdated and unhelpful.[261] Courts understanding this have questioned the government's assertion that blanket removal of electronic data is always necessary. Specifically, Judge King in the District of Oregon found that the agent's assertion that the computers would need to be searched off-site "may not always be true due to technological developments. . . . Had there been any evidence that a number of suspect computers would be found on site, there may well be an obligation to use a program like ENCASE to more narrowly tailor the search and seizure."[262]

For all of these reasons, requiring the government to disclose the actual risks of a computer search to justify the extraordinary measure of over-seizure is supportable.

D. Designing Search Protocols

CDT's fourth guideline instructs the government to design a search protocol to uncover only the information for which it has probable cause.[263] This guideline, similar to the use of a segregation team, addresses the sorting and separating of the seizable data described in the warrant from the commingled data swept up in the over-seizure. The

[257] McLain, *supra* note 59, at 1081.

[258] *Id.* at 1084.

[259] *Hill*, 459 F.3d at 974.

[260] *Id.*

[261] McLain, *supra* note 59, at 1082–83. Similarly, courts often justify broad seizures based upon the myth that users can adequately disguise files by manually changing the file extension, as for example, saving a Word file with an image extension, like "letter.jpg." However, forensic software like EnCase includes a feature that identifies mismatched file extensions, undermining this argument. *Id.* at 1095.

[262] United States v. Greathouse, 297 F. Supp. 2d 1264, 1275 (D. Or. 2003); *see also* Jekot, *supra* note 65, at *43 (arguing that on-site searches are feasible with forensic software in some cases and that police only need to look at certain classes of data, and not all data, which can be sorted out by forensic software).

[263] *CDT En Banc*, 579 F.3d 989, 1006 (9th Cir. 2009).

court asserted, "if the government is allowed to seize information pertaining to ten names, the search protocol must be designed to discover data pertaining to those names only, not to others, and not those pertaining to other illegality."[264] Once the data is segregated, the case agents can review only the data specified within the warrant.[265]

Courts and commentators alike have discussed whether or not the Fourth Amendment compels court-mandated search protocols within the digital evidence context. Three main views exist: (1) nothing in the language of the Fourth Amendment, or in the jurisprudence of the Supreme Court, requires such a rule;[266] (2) to meet the particularity requirement, a search of a computer requires the government to specify a search strategy within the warrant application;[267] and (3) in some cases, an *ex ante* strategy may be necessary to comport with the Fourth Amendment.[268]

1. No Support for Requiring Search Protocols

In his dissent in *CDT*, Judge Callahan criticized the search protocol guideline as overbroad and unsupported.[269] Moreover, Judge Callahan pointed out that the guidelines contradict earlier opinions that cautioned against affording computer searches heightened Fourth Amendment protections.[270] Specifically, the Ninth Circuit came to the opposite conclusion just three years earlier in *Hill*.[271] Indeed, the determination in *Hill* sums up the majority view: "we look favorably upon the inclusion of a search protocol; but its absence is not fatal."[272]

The courts and commentators advocating this view often cite the Supreme Court case *Dalia v. United States*.[273] In this case, the government suspected Dalia of conspiring to transport, receive, and possess stolen goods and obtained authorization to install electronic eavesdropping

[264] *Id.* at 999. In its discussion of search protocols, the court took special care to explicitly forbid the use of hashing tools absent probable cause. Therefore, law enforcement cannot simply search bitstream copies for well-known illegal files (such as child pornography) without probable cause to believe such files would be found. *Id.*

[265] *Id.* at 1000.

[266] *See, e.g.*, United States v. Graziano, 558 F. Supp. 2d 304, 315 (E.D.N.Y. 2008) (citing Dalia v. United States, 441 U.S. 238, 257 (1979)); *see also* Clancy, *supra* note 13, at 218–19 (referencing *Dalia*).

[267] *See, e.g.*, *In re* 3817 W. West End, 321 F. Supp. 2d 953, 961 (N.D. Ill. 2004).

[268] *See, e.g.*, United States v. Burgess, 576 F.3d 1078, 1091 (10th Cir. 2009).

[269] *CDT En Banc*, 579 F.3d at 1013 (Callahan, J., concurring in part and dissenting in part).

[270] *Id.*

[271] United States v. Hill, 459 F.3d 966, 978 (9th Cir. 2006).

[272] *Id.*; *see also* United States v. Farlow, No. CR-09-38-B-W, 2009 WL 4728690 at *5 (D. Me. Dec. 3, 2009) (quoting the magistrate judge issuing the warrant: "[i]mposing a search protocol . . . is something that a judge may do. . . . However, I cannot say . . . the . . . failure to impose a search protocol . . . resulted in an overbroad warrant").

[273] 441 U.S. 238 (1979).

equipment in his business office.[274] Dalia moved to suppress the evidence obtained through the interception of conversations in his office, contending that because the court did not explicitly authorize a covert entry under the terms of the surveillance, the entry violated his Fourth Amendment privacy rights.[275] The Court rejected this argument, holding that the Fourth Amendment warrant requirement necessitates only three things: (1) issuance by a detached and neutral magistrate; (2) probable cause; and (3) a particular description of the things to be seized and the place to be searched.[276] Moreover, "[n]othing in the language of the Constitution or in this Court's decisions interpreting that language suggests that, in addition to the three requirements[,] . . . search warrants also must include a specification of the precise manner in which they are to be executed. On the contrary, it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant."[277]

The DOJ Manual takes the position that court mandated search protocols are unnecessary because case agents and investigators are already subject to constitutional restrictions.[278] The Fourth Amendment controls a search warrant's execution by *ex post* judicial review of the reasonableness of the search.[279] Upon closer examination, the guidelines which seem to be imposed upon the execution of the warrant really function as factors within the reasonableness inquiry. To illustrate, in execution of search warrants in homes, there is a "knock and announce" requirement. This describes the common-law obligation of police to knock and announce their presence before entering someone's home to execute a search warrant.[280] However, the Supreme Court has specified that there is no rigid rule requiring an announcement in all instances[281] and that "[t]he Fourth Amendment's flexible requirement of reasonableness should not be read to mandate a rigid rule of announcement that ignores countervailing law enforcement interests."[282]

With this as a backdrop, most courts agree that warrants authorizing the search of electronic storage devices need not specify a search protocol. For example, in *United States v. Brooks*, the Tenth Circuit declined to find a search warrant insufficiently particular because it failed to describe a specific search methodology for the computer search.[283] In

[274] *Id.* at 241–42.

[275] *Id.* at 255.

[276] *Id.*

[277] *Id.* at 257.

[278] DOJ MANUAL, *supra* note 54, at 80.

[279] *See* United States v. Ramirez, 523 U.S. 65, 71 (1998); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 652–53 (1995).

[280] *See Ramirez*, 523 U.S. at 70; United States v. Banks, 540 U.S. 31, 41 (2003).

[281] *Ramirez*, 523 U.S. at 70.

[282] Wilson v. Arkansas, 514 U.S. 927, 934 (1995).

[283] 427 F.3d 1246, 1252 (10th Cir. 2005).

Brooks, the defendant challenged a third search warrant authorizing a laboratory search of his computer for child pornography on the grounds that the absence of a search protocol violated the particularity requirement by allowing investigators to search through text files that may not have included child pornography images.[284] Unpersuaded, the court clarified that warrants need not specify a search methodology and require only a particular description of the objects of the search.[285] Similarly, the Eighth Circuit acknowledged that although at times a search methodology may be useful, its absence does not render a search warrant invalid per se.[286]

In addition, numerous practical problems exist in developing search protocols for the magistrate judge to approve. First, a search of an electronic storage device is "as much an art as a science,"[287] and the ability to create a search strategy is contingent upon a number of factors that are at best difficult to predict and at worst impossible.[288] Even though, in *CDT*, a simple keyword search protocol to find the named players would have sufficed, computer searches are rarely so straightforward. In many cases, law enforcement often will not know what the forensic analyst will encounter on the storage device including the software used to create the evidence, the contents of the hard drive, or what steps, if any, the suspect or business has taken to protect or conceal files.[289] Second, the ability to articulate and approve a useful search strategy depends upon the technological acumen of the magistrate judge. Magistrate judges may have limited technical knowledge of computers and as a result, be "poorly equipped to evaluate whether a particular search protocol is the

[284] *Id.* at 1251.

[285] *Id.*

[286] United States v. Cartier, 543 F.3d 442, 447–48 (8th Cir. 2008); *see also* United States v. Roberts, No. 3:08-CR-175, 2010 WL 234719 at *17, *19 (E.D. Tenn. Jan. 14, 2010) (finding that lack of a written search methodology does not violate the Fourth Amendment by citing *United States v. Khanani*, 502 F.3d 1281, 1290–91 (11th Cir. 2007), which it summarized as "holding that lack of a written search methodology did not require suppression, particularly when agents took precautions to search only those computers and analyze only those files that were likely to contain items within the scope of the search warrant"); United States v. Farlow, No. CR-09-38-B-W, 2009 WL 4728690 at *6 (D. Me. Dec. 3, 2009) (determining that search protocols should be examined by the courts *ex post* to determine whether the police stayed within the authorized parameters and complied with constitutional standards); United States v. Graziano, 558 F. Supp. 2d 304, 315 (E.D.N.Y. 2008) (ruling that a warrant not containing a search methodology is not facially overbroad).

[287] United States v. Brooks, 427 F.3d 1246, 1252 (10th Cir. 2005).

[288] *See* Kerr, *supra* note 55, at 570, 575. No "Perfect Tool" exists that "efficiently searches a computer hard drive, returning only the evidence sought."*Id.* at 570; *see also* United States v. Burgess, 576 F.3d 1078, 1093 (10th Cir. 2009) (explaining how "[i]t is unrealistic to expect a warrant to prospectively restrict the scope of a search by directory, filename or extension or to attempt to structure search methods—that process must remain dynamic").

[289] Kerr, *supra* note 55, at 575–76.

. . . most targeted way of locating evidence" on a digital storage device.[290] In fact, poorly equipped magistrates and reviewing judges may rely upon specific protocols that are outdated or which may hamper law enforcement's ability to adapt to changes in criminal methodology.[291] Third, crafting generic protocols in response to these difficulties may only lead to boilerplate language that "unnecessarily requires law enforcement officers to state . . . unchanging fact[s] with every computer search warrant application, and yet fails to protect individual privacy."[292]

2. Support for Requiring Search Protocols

Before *CDT*, in the case *In re 3817 W. West End*,[293] the Northern District Court of Illinois refused to issue a warrant that did not include a computer search protocol. In this case, the government sought a warrant to search a home for evidence of federal income tax fraud.[294] The warrant contained a condition requiring the government to provide a search protocol describing the information the government sought to seize from the computer and "the methods the government planned to use to locate that information without generally reviewing information on the computers that was unrelated to the alleged criminal activity."[295] After seizing numerous computer disks, the government requested the court to allow a search of the electronic data without providing a protocol, but the court refused.[296] Similarly, a district court in Utah suppressed documents seized from the defendant's computer, concluding that once agents learned of the presence of intermingled documents on the computer, the agents should have presented a search methodology to support a more specific warrant.[297]

In reaching these decisions, both courts recognized the qualitative differences between electronic and physical data. First, when law enforcement requests a broad seizure of data, the normal sequence of a search followed by selective seizure is "turned on its head."[298] Second, unlike the review of paper documents, computer technology provides

[290] *Id.* at 575; *see also Farlow*, 2009 WL 4728690 at *6 n.3 (criticizing *CDT* guidelines as unworkable, stating "[e]ven the most computer literate of judges would struggle to know what protocol is appropriate in any individual case").

[291] McLain, *supra* note 59, at 1101.

[292] *Id.* at 1072.

[293] 321 F. Supp. 2d 953 (N.D. Ill. 2004).

[294] *Id.* at 954–55.

[295] *Id.* at 954.

[296] *Id.*

[297] United States v. Barbuto, No. 2:00CR197K, 2001 WL 670930, at *4–5 (D. Utah Apr. 12, 2001); *see also* People v. Gall, 30 P.3d 145 (Colo. 2001). In this case, a Colorado Supreme Court justice wrote a lengthy dissent declaring that "a warrant must include measures to direct the subsequent search of a computer's data." *Id.* at 160 (Martinez, J., dissenting). Thus, a warrant could specifically direct the search of the computer's contents or it could require a more detailed search warrant prior to any such search.

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

numerous methods to tailor the search of electronic data.[299] Generally, law enforcement can outline the methods they will use to sift through the electronic data before the magistrate approves the warrant application.[300] For example, libraries of hash values[301] exist for common programs and files and can be used by analysts to separate the important information from the unimportant. An investigator not interested in word processing software can use the hash value for this program to exclude it from his review.[302] In some situations, investigators can use keyword searches to determine if documents fall within the scope of the warrant.[303] Of course, not every search will lend itself to a particular search method.[304] Nevertheless, because the technology exists to limit the scope of what law enforcement either seizes or reviews after over-seizure, the *West End* court found a generic description of how the government intends to search a computer insufficient to meet the Fourth Amendment's particularity requirement.[305]

Additionally, contrary to what some commentators and courts believe, judges often understand the basic technology underlying search protocols. In most cases, the technologies involved are not especially complicated and expert testimony or amicus briefs can adequately

[299] *Id.* at 959 ("These methods include limiting the search by date range; doing key word searches; limiting the search to text files or graphics files; and focusing on certain software programs. . . . [T]he existence of these tools demonstrates the ability of the government to be more targeted in its review of computer information than it can be when reviewing hard copy documents in a file cabinet.").

[300] Winick, *supra* note 126, at 107.

[301] Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 HARV. L. REV. F. 38, 39 (2005), *available at* http://hlr.rubystudio.com/media/pdf/salgado.pdf ("Hashing is the process of taking an input data string (the bits on a hard drive, for example), and using a mathematical function to generate a (usually smaller) output string. For example, one could take a digital wedding photo from a hard drive and calculate the hash value of the photo. Hash values can also be calculated for other data sets, including the contents of a DVD, USB drive, or an entire hard drive.").

[302] *Id.*

[303] *In re* Grand Jury Subpoena *Duces Tecum* Dated Nov. 15, 1993, 846 F. Supp. 11, 13 (S.D.N.Y. 1994) (noting that the government had acknowledged that use of a key word search would have been sufficient to locate documents relevant to the investigation); Susan W. Brenner & Barbara A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 MICH. TELECOMM. & TECH. L. REV. 39, 60–61 (2002).

[304] "The usefulness of keyword searches is further diminished by the fact that such searches are context insensitive." Brenner & Frederiksen, *supra* note 303, at 61. The DOJ Manual also notes how some types of files cannot be searched for keywords, particularly TIFF and some PDF files. DOJ MANUAL, *supra* note 54, at 79. *See also* United States v. Vilar, No. S305CR621KMK, 2007 WL 1075041 at *38 (S.D.N.Y. Apr. 4, 2007) (finding that confining a computer search by a key-word search protocol would immunize criminals by leaving out encoded documents, documents using acronyms or other abbreviations in place of the "key words," and documents that are not word-searchable).

[305] *In re* 3817 W. West End, 321 F. Supp. 2d 953, 960–61 (N.D. Ill. 2004).

explain what is involved to the judge.[306] Notably, it was the government in *West End* that displayed a lack of technological savvy. Specifically, when the district court judge asked the government technical expert about examining the "metadata" in the computer files, the expert had "no response, leaving the court with the firm impression that he was not familiar with a term that [they] would expect a computer expert to know."[307]

Finally, not requiring a search protocol allows the government to argue and employ its own "special approach" for computer searches, which often works solely to the advantage of law enforcement. For example, the government routinely argues that the nature of electronic data requires over-seizure and off-site examination.[308] Yet, the government also argues against taking a special approach to limit computer searches in order to better protect individuals' Fourth Amendment rights. Without search strategies outlined ahead of time, "officers have the broad discretion to set the parameters for their own search."[309] More significantly, if officers are allowed to cursorily examine the contents of each file in order to determine if a given document is within the scope of the warrant, an individual's protection depends upon police officers policing themselves.[310] Thus, requiring an *ex ante* strategy ensures that the search will not exceed constitutional bounds, and it may be the most effective means of protecting individual rights within the computer search context.

3. When a Search Strategy May Be Necessary

Other courts leave open the possibility of requiring search protocols in certain cases. In *United States v. Cartier*, the Eighth Circuit refused to find that the absence of a search protocol rendered a search warrant invalid per se, yet acknowledged that "there may be times that a search methodology or strategy may be useful or necessary."[311] In *Cartier*, investigators searched thirteen hard drives, two thumb drives and hundreds of compact disks seized from the defendant, suspected of possessing child pornography.[312] Cartier argued that the absence of a search protocol rendered the warrant invalid per se.[313] However, he failed

[306] Solove, *supra* note 240, at 771–72.

[307] *In re 3817 W. West End*, 321 F. Supp. 2d at 956 n.1; *see also* United States v. Kim, 677 F. Supp. 2d 930, 950 (S.D. Tex. 2009). In this case, in its ruling to suppress evidence found within encrypted folders, the court adeptly discussed the encryption software Cryptapix and its use by the defendant and the government.

[308] DOJ MANUAL, *supra* note 54, at 76.

[309] Haynes, *supra* note 148, at 772.

[310] Trepel, *supra* note 51, at 137. Trepel raises significant doubts on the effectiveness of this reliance, particularly questioning "[z]ealous investigators motivated by the best of intentions" who then use the ends-justifies-the-means rationalization. *Id.* at 137–38.

[311] 543 F.3d 442, 447–48 (8th Cir. 2008).

[312] *Id.* at 445.

[313] *Id.* at 447.

to allege any harm suffered by the breadth of the search or any search of files unrelated to child pornography.[314] As a result, the court simply narrowly ruled that based upon the facts of the case, the absence of a search protocol did not undermine the validity of the warrant.[315] Importantly, the court's ruling does not foreclose the conclusion that under some circumstances, a search protocol may be necessary.

Similarly, the Tenth Circuit has also indicated *ex ante* strategies may be necessary in some situations. In *United States v. Burgess*, the court stressed the importance of conducting a search in such a way as to avoid the search of file types not identified in the warrant.[316] Specifically, the court stated that privacy rights require an officer to look first "in the most obvious places," and then if necessary, move from "the obvious to the obscure."[317] In this case, the officer used the software EnCase to search the defendant's computer for "trophy photos" relating to drug dealing and used the preview function to examine the files in a gallery view.[318] When the officer discovered images of child pornography, he immediately ceased his review of the files and secured a warrant to search the computer for child pornography.[319] Burgess challenged both the warrant authorizing the search of computer records and the scope of the search, contending that the officers violated the Fourth Amendment by failing to employ a search method that avoided searching files "which would not be related to any drug offense."[320] Although the court stated: "it is folly for a search warrant to attempt to structure the mechanics of the search and a warrant imposing such limits would unduly restrict legitimate search objectives," the court clarified that this does not mean search methodologies are irrelevant.[321] Notably, the court faulted the defendant for criticizing the search methodology as overbroad, but failing to offer an alternative.[322] In this situation, the court found the search reasonable because the officer's search was limited to image files, narrowly tailoring the ruling to particular facts of the case, perhaps indicating that under the correct circumstances and with a compelling argument from the defendant, a search protocol would be necessary.

---

[314] *Id.*

[315] *Id.* at 448.

[316] 576 F.3d 1078 (10th Cir. 2009).

[317] *Id.* at 1094. For example, the court suggested using a search protocol analyzing the file structure, then looking for suspicious file folders and using a keyword search of the types of files most likely to contain the evidence sought. *Id.*

[318] *Id.* at 1084. "Trophy photos" within this context are photos displaying cash and drugs. The gallery view of EnCase provides an option where multiple reduced-size photos are displayed on one page.

[319] *Id.*

[320] *Id.* at 1090, 1092.

[321] *Id.* at 1094.

[322] *Id.* at 1095. See also the Tenth Circuit's criticism in *United States v. Brooks*, 427 F.3d 1246, 1251 (10th Cir. 2005) ("[N]or has Brooks suggested how the search in this case would have been different with a scripted search protocol.").

Ultimately, until courts become comfortable with the existence of accurate search strategies that "would protect [an individual's] legitimate interests and also permit a thorough search for evidence,"[323] computer search protocols should be viewed as a part of "a 'best practices' manual, rather than binding law."[324]

VI. GOING FORWARD—VIEWING THE *CDT* GUIDELINES AS A TOOLBOX

Notwithstanding the constitutional questions the *CDT* guidelines raise, imposing all four of the guidelines discussed in this Note may prove both unnecessary and excessive. Indeed, Judge Kozinski suggested the court need not employ all of the guidelines. For example, he instructs that if the government does not consent to a waiver of the plain view doctrine in the warrant application, then the magistrate should order the separation of the seizable from the non-seizable data by an independent segregation team.[325] Additionally, imposing all of the guidelines in each situation may not only be impractical, but excessive. Using the facts in *CDT* as an example, forswearing the plain view doctrine alone would have protected the third party drug testing results from being used to apply for additional warrants. In the same way, requiring a segregation team to first segregate the data likely would have kept information outside the scope of the warrant away from the prosecution team. After forswearing the plain view doctrine and using a segregation team, it is difficult to determine what added protection a search protocol offers.

The guidelines also address distinct fundamental privacy concerns at different stages of the search. In particular, forswearing the plain view doctrine and the use of segregation teams function as *ex post* strategies—used after the search has occurred. Neither reduces the invasiveness of the search nor prevents it from becoming a de facto general search. Rather, forswearing plain view and segregation teams limits the impact of such searches. Specifically, the use of a segregation team concentrates on limiting the access of the prosecution team to evidence outside the scope of the warrant. In contrast, the guidelines suggesting disclosure of the actual risks of the search and crafting a search protocol operate as *ex ante* strategies which attempt to minimize the invasiveness of the search itself.

Finally, although the facts in *CDT* lent themselves easily to the creation of a search protocol, this is rarely the case. Consequently, it may be not only beneficial, but necessary, to view these guidelines as tools in a toolbox, where one guideline may work for one situation, but not in others. Re-organizing the guidelines reflecting their *ex ante* or *ex post*

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

[324] *CDT En Banc*, 579 F.3d 989, 1012–13 (9th Cir. 2009) (Callahan, J., concurring in part and dissenting in part).

[325] *Id.* at 998 (majority opinion).

application will also help. With that in mind, courts deciding to impose the *CDT* guidelines could update the language as follows:

> Before searching electronic storage devices, (1) "[Any] [w]arrants [or] subpoenas must disclose the actual risks of destruction of information as well as prior efforts to seize that information in other judicial fora;"[326] (2) If possible, the government should design a search protocol that will uncover only the information for which it has probable cause. If not possible, the government should be prepared to disclose the specific difficulties in doing so.
>
> Additionally, the court looks favorably upon *ex post* measures taken to limit the impact of an invasive search of electronic storage devices. If the government must make a blanket seizure of electronic data and cannot craft an adequate search protocol, then the magistrate should insist that the government waive reliance upon the plain view doctrine. The government bears the burden to justify the use of the plain view doctrine within the digital evidence context. As an alternative to forswearing the plain view doctrine, the government can employ a segregation team to segregate the responsive from the non-responsive data. If government personnel are used to segregate the data, the personnel must agree not to disclose to the case agents any information discovered that falls outside the scope of the warrant.

VII. CONCLUSION

The suggested guidelines in *CDT* boldly attempt to establish clear rules in a uniquely challenging area of law. The guidelines proposed are imperfect—not all supportable by case law and not all necessary or realistic to employ in every computer search. However, despite their shortcomings, several of the guidelines have enough support to be taken seriously in future fully briefed cases. Certainly, the *CDT* litigation (from the district court level to the final per curiam opinion) calls into question the plain view doctrine's application to the computer search context and sheds light on the dramatic results its application produces. In the continuing struggle to balance the needs of law enforcement and individuals' Fourth Amendment rights, the *CDT* guidelines provide courts valuable tools to help analyze the reasonableness of a computer search and, most importantly, keep the conversation moving forward.

[326] *Id.* at 1006.