Note

TIMOTHY C. CEDER*

The Guidelines of *Comprehensive Drug Testing, Inc.*: A Measured Approach?

Attempts by the judiciary to guide the search and seizure methodology of electronically stored information (ESI) have, until *Comprehensive Drug Testing* (*CDT*),[1] been conservative. Rather than announce sweeping reform to Fourth Amendment doctrine, the established procedures and rights associated with searches of physical documents have been applied piecemeal to the new paradigm, allowing the new medium to slowly be incorporated into the existing body of law. This practice would hopefully lead to computers being in the same position as file cabinets or sealed containers: just another wrinkle in the rules. However, the rapid technological shifts in ESI have outpaced the cautious movements of the courts, leaving the law governing searches of ESI in a woefully inadequate state.

The problem with ESI searches is simple: a computer belonging to or being used by the target of an investigation likely contains

* J.D. Candidate, University of Oregon. The author is a clerk at the U.S. Attorney's Office in Eugene, Oregon, and also works at the Lane County District Attorney's Office. He will graduate with a Criminal Law Certificate in December 2010. The author would like to thank Sean Hoar, Erin Gould, Carrie Leonetti, his parents, and his sister, all of whom provided unconditional guidance and inspiration during the writing of this Note.

[1] United States v. Comprehensive Drug Testing, Inc. (*CDT*), 579 F.3d 989 (9th Cir. 2009) (en banc).

information relevant to an ongoing investigation, but the same computer may also store information that is irrelevant to the investigation and that has no criminal implications. Nevertheless, the computer is seized and the relevant information is found, but in the course of searching the computer, the examiner stumbles upon information that falls into the area between the two extremes: irrelevant to the investigation but incriminating nonetheless. The law must balance the right to privacy of the nontarget against the need for criminal punishment, but how should it do so?

The traditional solution has been to treat computers as being analogous to physical document storage, such as file cabinets. Under this method, once the incriminating information is in "plain view," it is fair game for evidentiary purposes. But unlike traditional searches, computers have the ability to house not only one person's vast quantities of data, but thousands or millions of uninvolved third-party individuals' data, as well. For example, imagine a file cabinet that contained a small number of documents that were nonresponsive and some that were responsive. Because the numbers are relatively small, the documents could be quickly sorted. A computer, on the other hand, may have only one document that is responsive and millions that are not; thus, the potential for an invasion of privacy is far greater.

The Ninth Circuit, which is the only circuit thus far to require a specific search protocol in ESI searches,[2] purports not only to identify this difficult issue and its nuances but also to solve it with the sweeping guidelines issued in the *CDT* decision.[3] These guidelines, which are described in Part II, lay out the Ninth Circuit's expectations for the future of ESI searches.

There are several valid criticisms of the *CDT* guidelines. First, the Ninth Circuit apparently reached beyond its Article III duty in issuing the *CDT* guidelines. *CDT* presented several questions to the court, primarily whether one particular appeal was timely filed and whether

[2] Other circuits have addressed this issue but have not required specific protocols. *See generally* United States v. Burgess, 576 F.3d 1078 (10th Cir. 2009) (holding that a search protocol requirement is unrealistic); United States v. Cartier, 543 F.3d 442 (8th Cir. 2008) (declining to require a blanket protocol); United States v. Khanani, 502 F.3d 1281 (11th Cir. 2007) (holding that a warrant should not have included a search protocol); United States v. Upham, 168 F.3d 532, 537 (1st Cir. 1999) ("The warrant process is primarily concerned with identifying *what* may be searched or seized——not how . . . .").

[3] *CDT*, 579 F.3d at 989.

another appeal was controlled by the preclusive effect of two district court orders.[4] However, the court took "the opportunity to guide our district and magistrate judges in the proper administration of search warrants."[5] It is easy to see how such a statement can be read as the court's issuing an advisory opinion, a practice that is simply not allowed.[6] Second, the *CDT* guidelines conflict with controlling authority. This criticism is based on the *CDT* decision's attempt to limit the extensively developed and well-settled doctrine of plain view.[7] Also, *CDT*'s additional warrant requirements conflict with both existing precedent and the Federal Rules of Criminal Procedure. Third, the guidelines are unworkable. Their implementation seriously compromises the ability of the government to effectively investigate crimes and successfully prosecute criminals because they limit the tools available to investigators.

This Note analyzes the *CDT* guidelines in five parts. Part I briefly reviews the facts of the case to provide context to the guidelines and their intended application. Part II explains the basic governing law and concedes the point that the government failed to comply with that law. Part III explores how the decision impacts magistrate judges and affects their ability to issue warrants. Part IV discusses the government's ability to execute warrants after *CDT* and the guidelines' impact on cases thus far. Part V discusses whether *CDT* should be vacated or limited to methods that are implementable and founded on established law.

I
THE *CDT* DECISION AND THE GUIDELINES

In August 2002, federal authorities began investigating the Bay Area Lab Cooperative (BALCO) for allegedly distributing illegal steroids to Major League Baseball players.[8] In the same year, the Major League Baseball Players Association (MLBPA) reached an

4 *Id.* at 994.

5 *Id.*

6 Princeton Univ. v. Schmid, 455 U.S. 100, 102 (1982) ("We do not sit to decide hypothetical issues or to give advisory opinions about issues as to which there are not adverse parties before us.").

7 *See CDT*, 579 F.3d at 1006 ("Magistrates should insist that the government waive reliance upon the plain view doctrine in digital evidence cases.").

8 *Id.* at 993.

agreement with Major League Baseball (MLB) to provide urine samples of all players for suspicionless drug testing.[9] The agreement contractually obligated the players to provide urine samples for drug-testing purposes. However, all results were to be confidential and solely used to ascertain the pervasiveness of drug use in MLB.[10] The tests were performed by Quest Diagnostics, Inc., and all specimens were kept at Quest, but Comprehensive Drug Testing, Inc. (CDT) maintained a list of tested players and their respective results.[11]

In the course of its investigation, the government learned of ten players who had tested positive for steroids.[12] Based on the probable cause for the ten players and the knowledge that CDT maintained a list of all players' results, the government obtained a subpoena in the Northern District of California seeking "drug testing records and specimens" in CDT's possession for *all players*.[13] An effort was made to negotiate compliance, but these negotiations eventually broke down, prompting CDT and the MLBPA to move to quash the subpoena.[14] On the same day the motion was filed, the government obtained a warrant in the Central District of California to search CDT's facilities.[15] However, unlike the subpoena, this warrant was limited to the records of the *ten players* for whom there was probable cause.[16]

Included in the warrant was a provision to allow seizure of computer records from CDT for off-site examination and segregation of the evidence.[17] To justify this provision, which the government acknowledged would include information beyond that relevant to the investigation, the supporting affidavit contained an introduction that "explain[ed] the generic hazards of retrieving" ESI without any information specific to the actual case.[18] The court explained the warnings:

---

9 *Id.*

10 *Id.*

11 *Id.*

12 *Id.*

13 *Id.*

14 *Id.*

15 *Id.*

16 *Id.*

17 *Id.* at 995.

18 *Id.*

> In essence, the government explains, computer files can be disguised in any number of ingenious ways, the simplest of which is to give files a misleading name (pesto.recipe in lieu of blackmail.photos) or a false extension (.doc in lieu of .jpg or .gz). In addition, the date might be erased or hidden; there might be booby traps that "destroy or alter data if certain procedures are not scrupulously followed"; certain files and programs might not be accessible at all without the proper software . . . ; there may simply be too much information to be examined at the site; or data might be encrypted or compressed, requiring passwords, keycards, or other external devices to retrieve. The government also represented that "[s]earching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence."[19]

Based on these foreboding warnings, the magistrate granted the broad seizure. However, the warrant "contained significant restrictions on how the seized data were to be handled" to control the seizure, including review and segregation by non-investigating law enforcement personnel instead of the case agents.[20] This segregation was designed to provide the case agents with only those data for which probable cause existed.[21]

During the search of CDT's facilities, investigators found the "Tracey Directory," which included, among hundreds of other documents, an Excel spreadsheet containing the names of all players who had tested positive for steroids.[22] The searching agents determined that it would be impractical to sift through the information on-site, so they removed the data for off-site review, which was within the limits of the warrant.[23] Despite the inclusion of the segregation requirement in the warrant, the specifics of the warrant were largely ignored after seizure.[24] Rather than allow computer personnel to isolate the information authorized in the warrant, the case agent immediately took control of the data.[25]

Based on the information obtained by reviewing the Tracey Directory, the government obtained warrants to search the facilities of

---

[19] *Id.* (citations omitted).

[20] *Id.* at 995–96.

[21] *Id.* at 996.

[22] United States v. Comprehensive Drug Testing, Inc. (*CDT 2008*), 513 F.3d 1085, 1092 (9th Cir. 2008), *rev'd en banc*, 579 F.3d 989 (9th Cir. 2009).

[23] *Id.* at 1093.

[24] *CDT*, 579 F.3d at 996.

[25] *Id.* at 999.

CDT and Quest for information relating to *all players* and, in an apparent attempt to cover its tracks, issued subpoenas "demanding production of the same records it had just seized."[26] The acquisition of the additional inculpatory information was justified, the government claimed, based on the plain view observation of contraband.[27] CDT and the MLBPA moved for return of the seized property pursuant to Rule 41(g) of the Federal Rules of Criminal Procedure.[28] Two district court orders were issued requiring return of the property, although one allowed the government to retain the materials pertaining to the ten previously identified players.[29] The subpoenas were also quashed in a separate order.[30] All three of the presiding judges were unimpressed by the government's behavior.[31]

Despite the firm rebuke by the lower court, the government appealed to the Ninth Circuit, where a panel decision was issued, withdrawn, and reissued.[32] The panel reversed two of the lower courts' orders to return the property because the MLBPA had based its challenge to the search on the grounds that the seizure was illegal.[33] However, the panel also held that the government had failed to timely appeal the third order, binding the government to that order's factual determinations. These facts included the government's failure to comply with the warrant and case law conditions and that it had "displayed a callous disregard for the rights of third parties."[34] Nevertheless, the end result was that the seizure was upheld. The dissent vigorously disagreed with the decision, claiming, among other things, that the decision was unfounded, ignored factual findings of the lower courts, and would have dire ramifications.[35]

---

[26] *Id.* at 993.

[27] *Id.* at 998; *CDT 2008*, 513 F.3d at 1095.

[28] *CDT*, 579 F.3d at 993.

[29] *Id.* at 994.

[30] *Id.*

[31] *Id.*

[32] Derek Regensburger, *Comment: The Ninth Circuit's En Banc Ruling in United States v. Comprehensive Drug Testing, Inc. Sets New Rules for Computer Searches, but for How Long?* 2 (2009) (*available at* http://works.bepress.com/derek_regensburger/2).

[33] *CDT 2008*, 513 F.3d 1085, 1113 (9th Cir. 2008), *rev'd en banc*, 579 F.3d 989 (9th Cir. 2009).

[34] *CDT*, 579 F.3d at 995.

[35] *CDT 2008*, 513 F.3d at 1116–17 (Thomas, J., concurring in part and dissenting in part).

MLBPA appealed the panel decision, and a rehearing en banc was granted, ironically, with none of the judges who had appeared on the initial panel sitting.[36] Here, the positions taken in the earlier panel decision switched; the majority issued a scathing criticism of the government and ordered the property returned while the dissent warned of dire ramifications.[37] The en banc panel reversed the previous panel decision and ordered return of the testing results for all but the ten athletes for whom there had originally been probable cause.[38] The decision was based primarily on issue preclusion—because the government was bound by the factual determinations of the order that it failed to timely appeal, the issues contained in the government's appeal were already conclusively resolved.[39] Thus, the determination by the en banc panel was largely based on procedural grounds, and the holding required the government to return all seized data not pertaining to the original ten players.

"Had the court stopped there, this ruling would have been unremarkable," [40] but the court reached far beyond the issues presented in the appeal. The court went to great lengths to explore the underlying issues in the government's improper behavior. Throughout the opinion and especially in a section titled "Concluding Thoughts," the court explained that, although "[w]rongdoers and their collaborators have obvious incentives to make data difficult to find, . . . parties involved in lawful activities may also encrypt or compress data for entirely legitimate reasons."[41] In light of this, the interests of innocent parties to keep their stored information private must be balanced against the legitimate need of law enforcement to sweep up large quantities of data and sift through them for "concealed or disguised pieces of evidence."[42] In this process, the government agent reviewing the data could come across vast quantities of incriminating information that it could then claim fell into the plain view exception.[43] Thus, in the absence of any limitations, there is a risk that any warrant for the limited seizure of ESI would

36 *CDT*, 579 F.3d at 994.

37 *See id.* at 1005–07.

38 *Id.* at 1003.

39 *Id.* at 997.

40 Regensburger, *supra* note 32, at 2.

41 *CDT*, 579 F.3d at 1004.

42 *Id.*

43 *Id.* at 1004–05.

automatically become a general warrant for any data storage that is connected physically or digitally.[44] The Court further speculated that any ESI warrant could justify the search of "computers many miles away, on a theory that incriminating electronic data could have been shuttled and concealed there."[45]

To address the perceived risks of limitless warrants, the court created a set of five guidelines that it hoped would "prove a useful tool for the future."[46] In the majority's view, the guidelines strike a "delicate balance" in preserving constitutional freedoms and allowing prosecution of criminal activity.[47] The court summarized the guidelines as follows:

> 1. Magistrates should insist that the government waive reliance upon the plain view doctrine in digital evidence cases.
> 2. Segregation and redaction must be either done by specialized personnel or an independent third party. If segregation is to be done by government computer personnel, it must agree in the warrant application that the computer personnel will not disclose to the investigators any information other than that which is the target of the warrant.
> 3. Warrants and subpoenas must disclose the actual risks of destruction of information as well as prior efforts to seize that information in other judicial fora.
> 4. The government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents.
> 5. The government must destroy or, if the recipient may lawfully possess it, return non-responsive data, keeping the issuing magistrate informed about when it has done so and what it has kept.[48]

As it turns out, the implementation of these guidelines has created a tremendous problem in investigations conducted since *CDT*.[49] The

[44] *Id.* at 1005 ("Authorization to search *some* computer files therefore automatically becomes authorization to search all files in the same subdirectory, and all files in an enveloping directory, a neighboring hard drive, a nearby computer or nearby storage media.").

[45] *Id.*

[46] *Id.* at 1006–07.

[47] *Id.* at 1007.

[48] *Id.* at 1006 (internal cross references omitted).

[49] *See, e.g.*, Hugh Kaplan & Christine Mumford, *Attorneys, Academics Sort Through Landmark Case on Computer Searches*, 85 Crim. L. Rptr. 688 (BNA) (Sept.16, 2009);

case is now briefed for a full-court en banc rehearing, which has only happened three times in Ninth Circuit history, and such a review has never been granted.[50] Despite the rehearing, these guidelines are currently good law in the Ninth Circuit and must be implemented and interpreted by courts. This Note will show just how difficult and impractical that task is.

II
PRELIMINARY CONSIDERATIONS: THE LAW AND THE GOVERNMENT'S FAILURE

Before exploring the ramifications of the *CDT* guidelines, a brief summary of the relevant law is warranted.[51] After a cursory review, it becomes apparent that the government failed to meet its obligations in this case (a point the author readily concedes). There are four areas of law that are especially relevant to understanding the impact of the *CDT* decision: the search warrant particularity requirement, the plain view doctrine, Rule 41 of the Federal Rules of Criminal Procedure, and the supervisory power generally.

A. Areas of Law Relevant to CDT

The Fourth Amendment requires that a warrant describe with particularity the area to be searched and the items or persons to be seized.[52] Though initially this may appear a substantial requirement, it does not extend far. For instance, the "particularity requirement does not include the conditions precedent to execution of the warrant," nor does it require that a property owner be given the warrant before a search is conducted.[53] Rather, the "Constitution protects property owners . . . by interposing, *ex ante*, the 'deliberate, impartial judgment of a judicial officer . . .' and by providing, *ex post*, a right to suppress evidence improperly obtained . . . ."[54] Exceptions

Orin Kerr, *The 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.

50 Regensburger, *supra* note 32, at 13.

51 These summaries are meant to introduce the reader to the law, but not to provide a fully fleshed-out view. As the analysis progresses in later Parts, the nuances of the law will be explained further and citations to further reading will be provided.

52 United States v. Grubbs, 547 U.S. 90, 97 (2006).

53 *Id.* at 98.

54 *Id.* at 99 (citing Wong Sun v. United States, 371 U.S. 471, 481–82 (1963)).

to the warrant requirement, such as the plain view exception, lessen the impact of even these modest protections.

Because of the unique qualities of computers, it is difficult to apply the plain view exception. As one author described them, computers are "[p]art workshop, part file cabinet, part stereo, and part diary."[55] Thus, there is no direct, historical plain view analogy that can be applied. The plain view exception applies when searching officers "have a warrant to search a given area for specified objects, and in the course of the search come across some other article of incriminating character."[56] When this occurs, items not particularly described in a warrant may be seized if (1) the officer was lawfully in a position from which to view the seized object, (2) the incriminating character of the object was immediately apparent, and (3) the officer had a lawful right of access to the object.[57] The second factor means that the officer has probable cause to believe the evidence is associated with criminal activity.[58] The doctrine has two major limitations: it cannot be utilized alone (i.e., in the absence of some legitimate search), and the discovery of evidence must be inadvertent.[59] Consideration of the subjective intent of the officer has been heartily rejected.[60]

Rule 41 of the Federal Rules of Criminal Procedure guides searches of ESI. This Rule, which was substantially amended on December 1, 2009,[61] several months after the en banc *CDT* decision, provides the requirements for a warrant, including specific provisions for ESI.[62] The Rule states that a magistrate judge "*must* issue the warrant if there is probable cause."[63] This language is unlike the language authorizing requests by telephone, which states that a

[55] David J.S. Ziff, *Fourth Amendment Limitations on the Execution of Computer Searches Conducted Pursuant to a Warrant*, 105 COLUM. L. REV. 841, 841 (2005).

[56] Horton v. California, 496 U.S. 128, 135 (1990).

[57] *Id.* at 134–35 (setting out the criteria for the plain view doctrine).

[58] *See* Minnesota v. Dickerson, 508 U.S. 366, 374–75 (1993); United States v. Stafford, 416 F.3d 1068, 1076 (9th Cir. 2005).

[59] *Horton*, 496 U.S. at 136 (quoting Coolidge v. New Hampshire, 403 U.S. 443, 468–69 (1971)).

[60] *Id.* at 129 ("[E]venhanded law enforcement is best achieved by applying objective standards of conduct, rather than standards that depend upon the officer's subjective state of mind.).

[61] *See* FED. R. CRIM. P. 41.

[62] *See id.* at (e)(2)(B).

[63] *Id.* at (d)(1) (emphasis added).

magistrate judge "*may* issue a warrant."[64] Thus, under Rule 41, once probable cause is established, the magistrate does not have the power to deny the warrant or to impose extra conditions, provided the contents of the warrant are sufficient. The Rule also notes that, "[u]nless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant."[65] Furthermore, when electronic storage media are seized, the inventory that must be returned to the court "may be limited to describing the physical storage media that were seized or copied."[66]

A final area of law relevant to *CDT* is the supervisory power of the courts. The supervisory power allows the court to impose rules of procedure and evidence on the inferior courts.[67] However, the supervisory power may not be used to either disregard or supplement binding case law[68] in a way that conflicts with constitutional or statutory provisions.[69] Rather, the power is intended only to allow guidance to lower courts in non-substantive areas. With these areas in mind, the problems with the *CDT* guidelines can be better understood.

B. Conceding the Point That the Government Erred

The *CDT* decision seems to reflect outrage at the actions of the government, and for good reason. The law that should have limited the case agent's behavior was in place, the warrant clearly demarcated the lines that could not be crossed and gave a generous process to retrieve relevant data, and there was plenty of breadth in the allowed seizures to further the investigation. However, even these boundaries were not enough to deter overreaching by the government.

As the factual recount in Part I illustrates, the government failed to follow the authorized procedures in this case. The most egregious failure is the immediate and unauthorized review of *all* the seized information by the lead case agent, which compromised the privacy of numerous third-party individuals.[70] The district judges below all

64 *Id.* at (d)(3)(A) (emphasis added).

65 *Id.* at (e)(2)(B).

66 *Id.* at (f)(1)(B).

67 Dickerson v. United States, 530 U.S. 428, 437 (2000).

68 United States v. Payner, 447 U.S. 727, 737 (1980) ("[A court may not] disregard the considered limitations of the law it is charged with enforcing.").

69 Thomas v. Arn, 474 U.S. 140, 148 (1985) ("Even a sensible and efficient use of the supervisory power . . . is invalid if it conflicts with constitutional or statutory provisions.").

70 *CDT*, 579 F.3d 989, 993 (9th Cir. 2009) (en banc).

"expressed grave dissatisfaction with the government's handling of the investigation, some going so far as to accuse the government of manipulation and misrepresentation."[71] On appeal, the government tried to explain its actions with the shaky logic that "the warrant didn't specify that *only* computer personnel could examine the seized files."[72] The en banc court was not impressed with this argument, stating that such a reading "would make a mockery of [precedent] and render the carefully crafted safeguards in the . . . warrant a nullity."[73] Their ire was fully revealed in the following hyperbolic example:

> Why stop at the list of all baseball players when you can seize the entire Tracey Directory? Why just the directory and not the entire hard drive? Why just this computer and not the one in the next room and the next room after that? Can't find the computer? Seize the Zip disks under the bed in the room where the computer once might have been. Let's take everything back to the lab, have a good look around and see what we might stumble upon.[74]

When facts such as those presented in *CDT* come before a court, it is not surprising that the court feels compelled to rectify the underlying issue. And for anyone to claim that the government did not wholly fail to observe its obligations would be arguing an untenable position. Despite the stance of this Note, the author fully acknowledges that mistakes were made in this case and that the return of the nonresponsive data was proper.

It should also be noted that *CDT* did establish some notable benefits for the future of ESI searches. First, the decision states clearly that the government may not rely on boilerplate language to justify searches but must "fairly disclose the *actual* degree of such risks in the case presented."[75] Such a statement serves as a powerful reminder that prosecutors may not simply assume that all investigations are the same, and it will hopefully increase the awareness of the needs of each individual investigation. Second, although the decision lacks any citation to Fourth Amendment precedent,[76] the requirement that plain view be waived, as opposed to

---

[71] *Id.* at 994.

[72] *Id.* at 1000.

[73] *Id.* at 998.

[74] *Id.*

[75] *Id.*

[76] *Id.* at 1017 (Bea, J., dissenting in part and concurring in part) (criticizing the guidelines as lacking any citation to the Supreme Court's Fourth Amendment precedent).

stating that it does not apply, implies that Fourth Amendment doctrines do apply to ESI searches. Third, there is an explicit acknowledgment that there is a "legitimate need to scoop up large quantities of data, and sift through it carefully for concealed or disguised pieces of evidence."[77] This recognition is important to ensure that warrants may continue to authorize over-seizure to be segregated later.[78]

However, any incremental furtherance of the understanding of an area of the law does not excuse a court's obligations to create laws that are constrained and balanced. A tired point rings true: bad facts make bad law. *CDT* presented a situation involving egregious government action, and the court responded proportionally. The next Parts of this Note will show why the guidelines that emerged were perhaps not the best.

III
THE INTERPLAY OF *CDT* AND ESTABLISHED LAW

The *CDT* decision imposes on magistrates several responsibilities that are simply beyond their warrant-issuing authority. The decision seems to adopt the theory that, because magistrates are responsible for compliance with the Fourth Amendment, magistrates have the constitutional authority to impose additional warrant requirements beyond those specifically listed in the Fourth Amendment or, for that matter, cases interpreting it.[79] However, that is not the case. In fact, the *CDT* guidelines lack foundation and conflict with much existing law.

A. Guidelines, Mandates, or Mandatory Guidelines?

It is unclear from the *CDT* decision whether the guidelines are meant to be advisory or mandatory. Throughout the opinion, the court makes remarks that suggest an unwillingness to force compliance:

> [W]e *trust* that the procedures we have outlined above will prove a useful tool for the future. In the end, however, *we must rely* on the

[77] *Id.* at 1004.

[78] *See, e.g.*, United States v. Hill, 459 F.3d 966 (9th Cir. 2006) (allowing a blanket seizure of all computer equipment).

[79] *See* Susan W. Brenner, *Internet Law in the Courts*, J. INTERNET L., Oct. 2009, at 18, 18.

> good sense and vigilance of our magistrate judges . . . . Nothing we could say would substitute for the sound *judgment* that judicial officers must exercise in striking this delicate balance.[80]

Thus, although the requirements seem to be binding, the magistrate's role remains the same: ensure that the ex parte nature of a warrant request is conducted in a way that protects the absent party's rights.[81] Juxtaposed to this tentative language are more demanding phrases implying that compliance is required, especially in the guidelines themselves, such as "[m]agistrates *should* insist" and "[s]egregation and redaction *must* be . . . done [and the government] *must* agree."[82] This failure to identify whether the guidelines are mandatory or merely advisory is frustrating and has immediately resulted in confusion as to whether prosecutors must comply. Reflecting this lack of articulation, the dissent states that the majority's "protocols are dicta and might be best viewed as a 'best practices' manual, rather than binding law."[83]

However, the guidelines were quickly treated as mandatory by issuing magistrates throughout the circuit. Emblematic of this is a letter from the Chief Magistrate Judge for the Western District of Washington that states: "we are all required to follow the requirements set forth in the [en banc panel's] decision."[84] The letter concludes that judges "will either modify or reject any provision that does not comply with [the *CDT*] requirements."[85] Other magistrates required the same.[86] Thus, regardless of the Court's intention, the ambiguity of *CDT* has resulted in lower courts' treating the guidelines as mandatory.[87]

---

[80] *CDT*, 579 F.3d at 1006–07 (emphasis added).

[81] Abraham S. Goldstein, *The Search Warrant, the Magistrate, and Judicial Review*, 62 N.Y.U. L. REV. 1173, 1178 (1987).

[82] *CDT*, 579 F.3d at 1006 (emphasis added).

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

[84] Letter from Karen L. Strombom, Chief U.S. Magistrate Judge, W. Dist. of Wash., to Robert Westinghouse, Assistant U.S. Attorney, U.S. Dep't of Justice 1 (Oct. 1, 2009) (on file with author).

[85] *Id.* at 2.

[86] Brief for the United States in Support of Rehearing En Banc by the Full Court at 5, United States v. Comprehensive Drug Testing, Inc., (Nos. 05-10067, 05-15006, 05-55354) (9th Cir. Nov. 23, 2009) [hereinafter Government's Brief] ("Magistrates and district court judges throughout this Circuit are treating the en banc panel's 'guidance' as binding.").

[87] *See also id.* at 6 ("[A] widespread consensus has emerged among judges throughout this Circuit that compliance is mandatory.").

B. Stepping Beyond the Issues Presented

The *CDT* decision presented the en banc court with several legal issues. Those issues related to the preclusive effect of district court orders, the timeliness of an appeal, compliance with various warrants, and abuses of discretion.[88] Noticeably absent from the issues presented is anything related to the warrant process itself. The dissent expressed concern, stating that "[t]he majority's prescriptions go significantly beyond what is necessary for it to resolve this case."[89] Rather than confining its opinion to the issues directly presented and briefed by the parties, the court issued an advisory opinion, which is not permitted of federal courts.[90] Advisory opinions are disallowed because they detract from courts' abilities to reach accurate results, as the adversary system must "rely on the parties to frame the issues for decision and assign to courts the role of neutral arbiter of matters the parties present."[91] It is interesting to note that mere weeks after the *CDT* opinion was issued, the Ninth Circuit remarked that "[o]ur role is neither to issue advisory opinions nor to declare rights in hypothetical cases, but to adjudicate live cases or controversies consistent with the power granted the judiciary in Article III of the Constitution."[92] Despite these constitutional limitations, the *CDT* decision reaches issues that were never briefed nor argued and were unnecessary to resolve the case before it. This overreaching caused Judge Bea, in dissent, to state that "the establishment of guidelines . . . in the manner chosen by the majority goes against the grain of the common law method of reasoned decision making, by which rules evolve from cases over time."[93]

---

[88] *Id.* at 3–4.

[89] *CDT*, 579 F.3d 989, 1012 (9th Cir. 2009) (en banc) (Callahan, J., concurring in part and dissenting in part); *see also* Government's Brief, *supra* note 86, at 3 (The court ventured "far beyond . . . and announc[ed] what purport to be, and are being understood as, binding guidelines for future cases involving computer searches.").

[90] *See* Preiser v. Newkirk, 422 U.S. 395, 401 (1975) ("[A] federal court has neither the power to render advisory opinions nor to decide questions that cannot affect the rights of litigants in the case before them.") (internal quotations and citations omitted).

[91] Greenlaw v. United States, 128 S. Ct. 2559, 2564 (2008); *see also* Princeton Univ. v. Schmid, 455 U.S. 100, 102 (1982) ("[Federal courts] do not sit to . . . give advisory opinions about issues as to which there are not adverse parties before [them].").

[92] Stormans, Inc. v. Selecky, 586 F.3d 1109, 1122 (9th Cir. 2009) (citation omitted).

[93] *CDT*, 579 F.3d at 1018 (Bea, J., concurring in part and dissenting in part).

C. Beyond the Supervisory Power's Power

It is also unlikely that the court has the ability to impose limitations on magistrates' ability to issue warrants. Presumably, any mandate would be rooted in the court's supervisory power, which allows the court to impose rules of procedure and evidence on the inferior courts.[94] This basis is presumed because the *CDT* decision is devoid of any meaningful reference to the source of its authority to impose guidelines on magistrate judges.[95] The supervisory power, while regularly invoked by courts to alter procedure to their ends, is certainly a difficult power to justify, and it is not surprising that the decision chooses to avoid explicit reference to this source.[96]

Assuming the supervisory power is the source of authority for imposing the *CDT* guidelines does not enhance their effectiveness. The Supreme Court has made it clear that the supervisory power cannot be used to supplement Fourth Amendment protections.[97] Plain view seizures, which *CDT* denies the government by requiring the doctrine be waived in ESI investigations,[98] are firmly rooted in Fourth Amendment jurisprudence and are well established as constitutionally permissible.[99] Indeed, the *CDT* decision acknowledges the application of the doctrine, but it is concerned about its application to ESI searches.[100] The Supreme Court has made clear that when officers "in the course of [a] search come across some other article of incriminating character," the plain view doctrine allows its seizure.[101] Thus, a seizure made pursuant to plain view is not a violation of a person's constitutional rights, and, therefore, it cannot be limited by the supervisory power. To do so "would amount

94 Dickerson v. United States, 530 U.S. 428, 437 (2000).

95 *See CDT*, 579 F.3d at 1013 (Callahan, J., dissenting in part and concurring in part) (stating that the guidelines are created "without citing to legal authority that would support these new rules"); Regensburger, *supra* note 32, at 3 ("Perhaps more surprising, however, was the complete lack of legal analysis offered for these sweeping new rules.").

96 *See generally* Amy Coney Barrett, *The Supervisory Power of the Supreme Court*, 106 COLUM. L. REV. 324 (2006) (exploring the nature, origin, and validity of the supervisory power).

97 United States v. Payner, 447 U.S. 727, 736 (1980).

98 *CDT*, 579 F.3d at 998.

99 Coolidge v. New Hampshire, 403 U.S. 443 (1971).

100 *See CDT*, 579 F.3d at 1004–05.

101 Horton v. California, 496 U.S. 128, 135 (1990).

to a substitution of [a lower court's] judgment for the controlling decisions of [the Supreme] Court."[102]

D. Conflicts with the Rule 41 Warrant Requirements

The *CDT* guidelines also directly conflict with the recently adopted Rule 41 of the Federal Rules of Criminal Procedure. Although *CDT* did not conflict at the time it was decided, a new Rule 41 was adopted about three months after the decision.[103] Because the Rules carry the force of the Supreme Court, all laws in conflict with the Rules have no further force or effect.[104]

The conflicts between the guidelines and Rule 41 are glaring. The *CDT* guidelines state "the government must provide the issuing officer with a return disclosing precisely what data it has obtained as a consequence of the search."[105] Meanwhile, for ESI seizures, Rule 41 states that "the inventory may be limited to describing the *physical storage media* that were seized or copied."[106] Thus, the two authorities conflict on what is required in an inventory of seized items. Similarly, *CDT* requires that, absent specific authorization otherwise, officers must return or destroy all copies of seized data[107] while Rule 41 states that "[t]he officer may retain a copy of the electronically stored information that was seized or copied."[108] This conflict, the logic of which is questioned in Part IV.B, is also direct. Once a rule of procedure is adopted, all laws in conflict with that rule have no further force or effect.[109] Thus, given that the *CDT* guidelines and Rule 41's requirements are in direct and unworkable

---

102 Government's Brief, *supra* note 86, at 9 (alteration in original) (quoting *Payner*, 447 U.S. at 737).

103 *See* FED. R. CRIM. P. 41.

104 *See* 28 U.S.C. § 2072(b) (2006) ("All laws in conflict with such rules shall be of no further force or effect after such rules have taken effect."); Clinton v. City of New York, 524 U.S. 417, 446 n.40 (1998) ("Congress itself made the decision to repeal prior rules upon the occurrence of a particular event—here, the promulgation of procedural rules by this Court.").

105 *CDT*, 579 F.3d at 1000–01.

106 FED. R. CRIM. P. 41(f)(1)(B) (emphasis added) (detailing the inventory requirement).

107 *CDT*, 579 F.3d at 1000 ("The government may not retain copies of such returned data, unless it obtains specific judicial authorization to do so.").

108 FED. R. CRIM. P. 41(f)(1)(B).

109 28 U.S.C. § 2072(b) (2006).

conflict, the former necessarily are deprived of their force in those areas that conflict.

Even if Rule 41 did not displace the *CDT* guidelines, the warrant requirement combined with Supreme Court precedent effectively contradicts the *CDT* guidelines with respect to the requirement of specifics in the search protocol. The guidelines require magistrates to make demands of the government beyond establishing probable cause. Nothing in the Constitution requires specificity in the manner of a warrant's execution; the particularity requirement applies only to what is searched and seized.[110] Efforts to expand the particularity requirement have been rejected.[111] A modicum of support can be found by claiming that the extra requirements ensure that privacy intrusions are minimized;[112] however, there is no suggestion that such safeguards are required or possible ex ante or that the traditional role of ex post review should be abandoned. Thus, the *CDT* guidelines seem to buck the established law by requiring more of the warrant process, despite the Supreme Court's "repeated[] refus[al] to declare that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment."[113]

The Tenth Circuit case of *United States v. Brooks* is exemplary of courts' study of the particularity requirement and an affirmation of its limits.[114] The appellant in *Brooks* claimed that a warrant that led to the discovery of child pornography on his computer was not sufficiently particular because it did not describe the search methodology to be employed.[115] The Court first enunciated that "the [particularity] requirement ensures that the search will be carefully tailored to its justifications, and [it] will not take on the character of the wide-ranging exploratory searches the Framers intended to

110 United States v. Grubbs, 547 U.S. 90, 97 (2006) ("[The Fourth Amendment] specifies only two matters that must be particularly describ[ed] in the warrant: the place to be searched and the persons or things to be seized.") (alteration in original) (internal quotations omitted). For a contrary view, see Brenner, *supra* note 79, at 18, which argues that magistrates can impose requirements on the government's execution of a warrant to ensure compliance with the Fourth Amendment.

111 *See* Dalia v. United States, 441 U.S. 238 (1979).

112 Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976) ("[R]esponsible officials, including judicial officials, must take care to assure that [searches for papers] are conducted in a manner that minimizes unwarranted intrusions upon privacy.").

113 Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 663 (1995).

114 United States v. Brooks, 427 F.3d 1246 (10th Cir. 2005).

115 *Id.* at 1251.

prohibit."[116] Beyond stating with particularity the "objects of their search," though, there is no requirement that seizing officers have a search protocol listed in the warrant.[117] The Tenth Circuit did make clear that in cases

> [w]here officers come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, the officers may seal or hold the documents pending approval by a magistrate. . . . The magistrate should then require officers to specify in a warrant which type of files are sought.[118]

This conclusion is logical as it enables officers specifically searching for evidence of a crime to undertake any means to find that evidence during their search, but it also limits officers should they stumble across irrelevant but incriminating material. Rather than try to limit the scope of the warrant by limiting the items, the scope is limited by subject matter.[119]

The *CDT* decision does not respect the same limits on the particularity requirement. Instead, it demands that particularity be employed in an area that, as Part IV explains, is not conducive to such ex ante descriptions.

IV
THE EFFECT ON LAW ENFORCEMENT

Prior to the *CDT* decision, there was leeway in warrants that facilitated investigations and led to convictions of parties who were, perhaps, not the initial target. Now, in response to *CDT*, former practices and procedures that were largely viewed as acceptable cannot be employed. In some U.S. Attorney's Offices, the guidelines have had a chilling effect on warrant applications or resulted in deferral to state authorities that are not bound by the requirements. This decreased ability to effectively execute warrants is a direct by-product of the guidelines.

---

116 *Id.* (quoting United States v. Riccardi, 405 F.3d 851, 863 (10th Cir. 2005)) (citing Maryland v. Garrison, 480 U.S. 79, 84 (1987)).

117 *Id.*

118 United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999) (citation omitted).

119 *See* United States v. Burgess, 576 F.3d 1078, 1091 (10th Cir. 2009).

A. Limitations on Off-Site Searching After CDT

One of the necessities of ESI searches is removal of the data storage device for off-site searching. After *CDT*, removal for off-site searching is still permitted, but it is severely restricted. The Ninth Circuit recognized that removal for off-site searches is already generally allowed by the showing of the impracticality of copying the data within a reasonable time without compromising the data.[120] The reasonable time considerations depend on several factual issues: size of memory, complexity of organization, encryption, passwords, type of documents sought, and resources available.[121] This allowance makes sense as officers executing a search warrant may have only a rudimentary understanding of computer technology; they may be unequipped to make advanced decisions regarding inculpatory materials.[122] Rather, their familiarity with computers may be like their familiarity with drugs: they know what is a crime but not the details.[123] The *CDT* guidelines require that any seized evidence that is nonresponsive to the warrant must be returned or destroyed within a time specified in the warrant, which should be as soon as practicable.[124]

However, this timeline fails to consider several issues. First, there is direct conflict with Rule 41, which allows the government to retain a copy of seized information.[125] Second, it ignores the reality that investigations often expand to include areas that were previously thought to be innocuous. If the government is unable to retain copies of seized media, there is a realistic fear that the later expansion of an investigation may be impossible if the evidence is no longer recoverable (such as when the defendant destroys the only copy). In

120 *CDT 2008*, 513 F.3d 1985, 1093 (9th Cir. 2008) *rev'd en banc*, 579 F.3d 989 (9th Cir. 2009).

121 Robert H. Bohn, Jr. & Lynn S. Muster, *The Dawn of the Computer Age: How the Fourth Amendment Applies to Warrant Searches and Seizures of Electronically Stored Information*, 8 SUFFOLK J. TRIAL & APP. ADVOC. 63, 72 (2003).

122 *See* Lanny L. Newville, *Cyber Crime and the Courts—Investigating and Supervising the Information Age Offender*, FED. PROBATION, Sept. 2001, at 11 (finding a deficiency in law enforcement's ability to investigate computer crimes).

123 *Id.* at 12.

124 *CDT*, 579 F.3d 989, 1000–01 (9th Cir. 2009) (en banc).

125 FED. R. CRIM. P. 41(f)(1)(B).

fact, "[t]he [state] is obligated to preserve exculpatory evidence."[126] Along the same lines, retaining a copy allows the government to prove that no information on the seized media was destroyed or not provided to the defendant in violation of the government's obligation under *Brady* to turn over exculpatory material.[127]

B. Misstatements of Technology and Misunderstandings of Ability

The *CDT* decision misunderstands the technology employed in searching ESI. In its decision, the court states that hashing tools exist that are sophisticated enough to allow searches without opening files.[128] Hash values are created by taking a known string of data bits and using a mathematical function to generate a value.[129] The created hash value cannot be reassembled into the file from which it was created; therefore, the hash value reveals nothing about the information in the original file itself.[130] The court, though, suggests that hashing tools could lead to a tailored search that is limited to only those files that meet the specific search criteria—in *CDT*, the ten players in the warrant.[131] However, because hashing tools allow an investigator to find only those files with known hash values, "hash calculations disclose nothing" about a file's contents.[132] Thus, the usefulness of hash values is confined to those instances where the values derived from seized files can be compared with the values from known contraband;[133] otherwise, the hash value is worthless. If the hashing tools were to be successfully employed in the *CDT* case, investigators would necessarily already have the files because they would need to derive the values from them for comparison. Furthermore, if the point of the *CDT* guidelines is to encourage the

126 Bohn & Muster, *supra* note 121, at 78 (discussing the need to preserve ESI evidence even after completion of a forensic search).

127 *See* Brady v. Maryland, 373 U.S. 83 (1963) (establishing that a prosecutor's withholding of exculpatory material violates the requirement of due process).

128 *CDT*, 579 F.3d at 999.

129 Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 HARV. L. REV. F. 38, 39 (2005).

130 *Id.* at 38–39.

131 *CDT*, 579 F.3d at 999.

132 Salgado, *supra* note 129, at 42.

133 For this reason, hash values are very useful in child pornography cases because there are known hash value sets (derived from known child pornography) to which the seized files' values can be compared. *Id.* at 45–46.

use of hashing tools, the result will be an increase in the invasion of privacy, as each matching value would reveal that a certain file was on the computer being searched, regardless of whether it is within the scope of the warrant.[134]

The court also demands that a specific search protocol be spelled out in the warrant affidavit.[135] While it is practical and required to include a methodology in the warrant pertaining to the segregation of relevant and innocuous data,[136] it is impossible to know beforehand what methods will be used to actually search for the relevant data.[137] It is interesting to note that the Ninth Circuit itself has acknowledged this reality: "[t]o require such a pinpointed computer search, restricting the search to [a particular] program or to specific search terms, would likely [fail] to cast a sufficiently wide net to capture the evidence sought."[138] As discussed in Part IV.D on decisions interpreting *CDT*, this is a difficult standard for courts to follow, and not just because of the magistrate's limited ability to evaluate the proper protocol.[139] It fails to recognize that the threats placed in a warrant, which the court refers to as part of a "strong generic case,"[140] could be present in any, all, or none of the electronic devices seized. In fact, a process of trial and error is often required to determine the structure and organization of files, including how a target may have hidden inculpatory files.[141] The simplest example of the inability to define a methodology beforehand is the inability to know if the encountered computer will be using a Windows, Apple, or Linux-based operating system. Because each operating system uses unique file structures, the methods are necessarily different; thus, in the absence of a generic contingency for all possibilities, spelling out the method is not feasible.

134 *Id.*

135 *CDT*, 579 F.3d at 999.

136 *See* United States v. Tamura, 694 F.2d 591, 595–96 (9th Cir. 1982).

137 *See* United States v. Brooks, 427 F.3d 1246, 1252 (10th Cir. 2005) ("[A] search can be as much an art as a science."); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 547 (2005) ("[D]ata acquisition refers to collecting the hay, and data reduction involves looking through the haystack for the needle.").

138 United States v. Adjani, 452 F.3d 1140, 1149–50 (9th Cir. 2006).

139 Kerr, *supra* note 137, at 575 ("[M]agistrate judges are poorly equipped to evaluate whether a particular search protocol is the fastest and most targeted way of locating evidence stored on a hard drive.").

140 *CDT*, 579 F.3d at 995.

141 Bohn & Muster, *supra* note 121, at 76–77.

The requirement of a specific search protocol also contradicts case law. In *Ex Parte United States*, the Supreme Court stated that a district court or a magistrate is prohibited from imposing restrictions on the issuance of a warrant once it is established that probable cause exists.[142] To require a specific protocol as a condition of the issuance of a warrant would be tantamount to requiring specificity in the manner of a warrant's execution, which the Supreme Court has specifically stated is unnecessary.[143] Rather, particularity is required only in describing the area to be searched and the evidence to be seized—"[n]othing in the language of the Constitution . . . suggests that, in addition to the requirements set forth in the text [of the Fourth Amendment], search warrants also must include a specification of the precise manner in which they are to be executed."[144]

C. The "Wall" Requirement

CDT also requires that the warrant application contain a provision prohibiting communication between the computer personnel and the investigators.[145] This requirement fails to recognize the level of sophistication present in many investigations, which often "seek particular information to answer more general questions, such as who used a computer, when they did so, and the purpose and manner of that use."[146] Computer forensics requires not just a mechanical search process for easily identifiable documents but an intuitive, on-the-spot judgment by the investigator of whether to pursue a particular avenue. Thus, information that may not appear readily related to the investigation to computer personnel may actually present useful facts that are relevant to the case investigators. This information can lead to other valuable information about a target's connections, movements, and behaviors, or about the beginning or ongoing nature of a crime. To connect the investigation to the seemingly innocuous material, the computer personnel must speak with the case agents lest important information be overlooked. The Ninth Circuit, however, simply cuts off all contact, regardless of its nature or relevancy, and assumes that misconduct is universal.

142 Ex Parte United States, 287 U.S. 241, 250 (1932); *see also* Goldstein, *supra* note 81.

143 United States v. Grubbs, 547 U.S. 90, 98 (2006).

144 *Id.* (quoting Dalia v. United States, 441 U.S. 238, 255 (1979)).

145 *CDT*, 579 F.3d at 1000.

146 Government's Brief, *supra* note 86, at 15.

The "no communication" requirement also strains government resources. For complicated cases, such as trafficking, fraud schemes, terrorism, and identity theft, compliance with the *CDT* guidelines would require that the segregating personnel become experts in the field of investigation.[147] This step may take months of additional training to enable computer personnel to reach the level of familiarity that a case agent has spent a career developing.[148] Additionally, the trained expert may not participate in the potentially ongoing investigation, which deprives case agents of the knowledge that the fully trained individual possesses. In short, the requirement demands that labor be divided between computer personnel and investigating agents, and the lack of crossover between the two essentially requires at least one extra person for every case involving ESI evidence.

The alternative suggested by the *CDT* decision is to farm out the segregation to a third party,[149] but this option also fails to consider several pitfalls. For instance, some materials may not be given to third parties. The Adam Walsh Act, for instance, which states that "[i]n any criminal proceeding, any property or material that constitutes child pornography . . . shall remain in the care, custody, and control of either the Government or the court."[150] Giving child pornography to a third party not associated with the government would therefore violate federal law. Furthermore, to fully understand the investigation and enable a reviewer to determine if information is responsive or not, other sorts of information may be needed. Some of this may be inappropriate or illegal to disseminate outside of law enforcement, such as grand jury testimony,[151] tax information,[152] or the results of court-ordered wiretaps.[153] Finally, evidence suppression, the traditional remedy for exceeding the scope of the

147 *Id.* at 16.

148 *See id.* at 6 ("[A]n FBI forensic examiner has advised that, to comply with the en banc decision's rules, he will need many months to learn a complex national security case before attempting to segregate responsive and non-responsive data on a seized computer.").

149 *See CDT*, 579 F.3d at 1000 ("At the discretion of the issuing judicial officer, and depending on the nature and sensitivity of the privacy interests involved, the computer personnel in question may be government employees or independent third parties not affiliated with the government.").

150 18 U.S.C. § 3509(m) (2006).

151 *See* FED. R. CRIM. P. 6(e).

152 *See* 26 U.S.C. § 6103(h)(2) (2006).

153 *See* 18 U.S.C. § 2517 (2006).

warrant, seems illogical when the misconduct comes from a non-law enforcement examiner. The *CDT* decision makes no mention of how this situation should be handled.

Another issue with utilizing third-party examiners is cost.[154] The dissent targets the increased expense required with either third-party examiners or the acquisition of new personnel, stating that "an agency would have to expand its personnel, likely at a significant cost, to include both computer specialists who could segregate data and forensic computer specialists who could assist in the subsequent investigation . . . . Both of these options would force law enforcement agencies to incur great expense . . . ."[155] The majority avoided this consideration, but the issue is real, and it threatens to further undermine already costly forensic practices. In short, the "wall" requirement is undermined by legitimate concerns that the *CDT* decision makes no effort to address.

D. Cases Interpreting CDT

Given the short time since the guidelines were announced, and the delay inherent in governmental response to them, there have been few decisions citing to *CDT*. Of the few decisions released, though, not one has been eager to enforce or adopt the guidelines. In *United States v. Cerna*, for instance, a court in the Northern District of California examined and rejected the defendant's complaint that "the government's search protocol . . . was inadequate."[156] There, the search protocol in the warrant "required the government to make 'all reasonable efforts' [to] mimimize[] exposure of irrelevant . . . or confidential files."[157] This was held to be "sufficiently tailored" to satisfy the *CDT* criteria, although the Court did not provide any insight into how it made that decision.[158] This inadequate explanation of what *CDT* actually requires will likely prove to be a

154 *See, e.g.*, Global Digital Forensics, GlobalDigital Forensics FAQ, http://www.evestigate.com/Computer%20Forensics%20FAQ.htm (last visited Oct. 2, 2010) (giving a price of $250–$350 per hour and a typical cost of $4500 for a fifteen-hour analysis).

155 *CDT*, 579 F.3d 989, 1013 (9th Cir. 2009) (en banc) (Callahan, J., dissenting in part and concurring in part).

156 United States v. Cerna, No. CR 08-0730 WHA, 2009 WL 5125920, at *7 (N.D. Cal. Dec. 21, 2009).

157 *Id.*

158 *Id.*

recurring theme in lower court decisions given that there is so little indicia of intent in the *CDT* opinion. Without a body of case law supporting the guidelines, lower courts cannot know the contours of the law; therefore, they will simply choose "yes" or "no," without adequately explaining their decisions until that case law develops.[159]

Another recent opinion held that the *CDT* guidelines are not immune from the good faith exception.[160] In *King*, the court issued a warrant to search a defendant's computer and peripherals for sex-trafficking evidence.[161] The warrant contained search protocols, and nothing seized went beyond the immediate investigation or was used as the basis for additional charges.[162] Nevertheless, the defendant asserted that the search did not explicitly comply with the *CDT* guidelines.[163] In refuting the assertion, the court stated, "the exclusionary rule should not apply to evidence seized in honest compliance with a warrant that comports with the Fourth Amendment but does not include all of the 'procedures' outlined in *CDT*."[164] Rather, the court took the view that the *CDT* guidelines are not necessarily based on the Fourth Amendment and should instead be viewed as best practices, and in any case, the good faith reliance on a warrant should preclude exclusion.[165]

Other circuits have refused to apply the *CDT* guidelines when confronted with the seizure of electronically stored information. In *United States v. Mann*, the Seventh Circuit criticized the decision and reiterated that the traditional remedy of suppression was appropriate.[166] In that case, a detective searched two of the defendant's computers on two separate occasions, separated by two months, for "images of women in locker rooms or other private

159 Or until *CDT* is amended or vacated. For another example, see *United States v. Seldon*, Nos. 09-10137, 09-10150, 2010 WL 2545897 (9th Cir. June 24, 2010), wherein the court states simply that the search procedures were complied with and the search did not move from "a limited search for particular information into a general search of office file systems and computer databases." *Id.* at *1 (quoting *CDT*, 579 F.3d at 998).

160 *See* United States v. King, 693 F. Supp. 2d 1200 (D. Haw. 2010).

161 *Id.* at 1127.

162 *Id.*

163 *Id.* Oddly, the opinion does not state what noncompliance occurred, and the "[d]efendant [did] not elucidate for the Court how the agents' search in the instant case . . . did not comply with *CDT* or the Fourth Amendment." *Id.* at 1227.

164 *Id.* at 1229–30.

165 *Id.* at 1223–24, 1230.

166 *See* United States v. Mann, 592 F.3d 779, 785 (7th Cir. 2010).

areas."[167] In both searches, the detective employed a "forensic tool kit" to convert all the images into a viewable format, which included listing "Known File Filter ("KFF") Alerts."[168] These KFF Alert files were flagged by the program because they matched files in a library of known contraband, mostly child pornography.[169] Both searches returned these results, which was sufficient evidence to obtain a second search warrant (for child pornography), but the detective failed to do so.[170] The defendant argued that the use of the child pornography images constituted an impermissible use of plain view and urged the court to apply the Ninth Circuit's rationale to find the search unconstitutional.[171] However, the court disagreed. Instead, it was "inclined to find more common ground with the [*CDT*] dissent's position," and it noted that there was no Supreme Court or Ninth Circuit case law justifying the abandonment of the plain view doctrine.[172] The court also stated that the better approach is "to allow the contours of the plain view doctrine to develop incrementally" through the normal adjudication process.[173] Finally, they expressed skepticism about the need "to always obtain pre-approval . . . to use the electronic tools necessary to conduct searches tailored to uncovering evidence that is responsive to a properly circumscribed warrant."[174]

In *United States v. Farlow*, a case from the District of Maine, the *CDT* guidelines were also rejected in favor of the traditional suppression remedy.[175] There, the search warrant authorized a search of electronic files for "evidence of the crimes of dissemination of indecent materials to minors or endangering the welfare of a

167 *Id.* at 781. The warrant specified that the search was for "video tapes, CD's [sic] or other digital media, computers, and the contents of said computers, tapes, or other electronic media, to search for images of women in locker rooms or other private areas." *Id.* at 780–81.

168 *Id.* at 781.

169 *Id.*

170 *Id.* at 781–82.

171 *Id.* at 785.

172 *Id.*

173 *Id.* (quoting *CDT*, 579 F.3d 989, 1013 (9th Cir. 2009) (en banc) (Callahan, J. concurring in part and dissenting in part)).

174 *Id.*

175 United States v. Farlow, No. CR-09-38-B-W, 2009 WL 4728690, at *6 (D. Me. Dec. 3, 2009).

child."[176] The defendant contended that the warrant was overbroad, but the court found otherwise, stating, "since the warrant stated the specific criminal activity likely to be found," it did not amount to an authorization for a general search in violation of the Fourth Amendment particularity requirement.[177] The court then acknowledged that if the *CDT* guidelines had been applied here, the evidence of child pornography would not have been found.[178] This is because the government would have been required to waive plain view and segregation of the responsive data would have screened out the child pornography.[179] The *Farlow* court disagreed with the Ninth Circuit approach. Instead, the court stated that:

> [T]he far preferable approach is to examine the circumstances of each case, to assess the validity of the computer search protocol, to determine whether the police strayed from the authorized parameters of the search warrant, and to hold the police to constitutional standards in the context of a *motion to suppress*.[180]

Should the police conduct be found to be egregious, as it was in *CDT*, then "the Court can consider appropriate remedies," such as suppression of some or all of the unconstitutionally seized evidence.[181] In a lengthy footnote, the court continued to pick apart the *CDT* guidelines, stating, "*CDT* creates more problems than it solves."[182] The focus here is on the extreme limitations that the Ninth Circuit placed on searches that will undoubtedly hinder investigations.[183] The court compared the relatively benign nature of the ill-gotten evidence in *CDT* (steroids) to the far more invidious evidence that plain view often uncovers (child pornography, terrorism).[184] In the court's view, the guidelines assume that

176 *Id.* at *4.

177 *Id.* at *4–5.

178 *Id.* at *6.

179 *Id.* (emphasis added).

180 *Id.*

181 *Id.*

182 *Id.* at *6 n.3.

183 *Id.*

184 *Id.* ("The judicial directive to forswear in advance the plain view doctrine, placed in a different context, is equivalent to demanding that a DEA investigative team engaged in the search of a residence for drugs promise to ignore screams from a closet or a victim tied to a chair.").

"misconduct will be the rule, not the exception" and that "at the very least the more traditional remedies should be tried first."[185]

Those courts that have utilized language from *CDT* to support a holding focus less on the guidelines and more on the Ninth Circuit's assessment based on individuals' rights. For instance, in *People v. Gutierrez*, a Colorado state court advocated an individualized approach when assessing whether suppression was appropriate following a questionable search.[186] In holding that probable cause was required for each individual involved in a search, the court used *CDT* as an example of an individualized approach to searches, stating that the expansion of the search from ten players to hundreds could not be justified based on probable cause for the original ten.[187] Similarly, in *SK Foods, L.P. v. Sharp*, the Eastern District of California used *CDT* only for the proposition that a reasonable expectation of privacy remains even if documents are intermingled.[188] This reluctance to adopt, or even endorse, the *CDT* guidelines illustrates the harsh reception of the sweeping reform demanded by the decision.

V

THE WAY FORWARD WITH A MEASURED APPROACH

The idea that third-party searches require a higher standard has also been rejected by the Supreme Court because "[t]he Fourth Amendment has itself struck the balance between privacy and public need."[189] Nevertheless, it is possible that a time has come where ESI is so prevalent and the risk of privacy invasion so high that a new approach is warranted. Perhaps a third party who is not the target of an investigation, like the other players in *CDT*, should be afforded greater protections than the actual target; but if this is true, the *CDT* guidelines should have been restricted to those cases involving innocent third parties and not all ESI seizures. In light of this, it

185 *Id.*

186 People v. Gutierrez, 222 P.3d 925, 940 (Colo. 2009) (en banc).

187 *Id.* at 938.

188 SK Foods, L.P. v. Sharp, No. 2:09-cv-02942-MCE, 2009 WL 5206639, at *3 (E.D. Cal. Dec. 24, 2009) ("Intermingling of documents, alone, does not waive Appellants' constitutional rights.").

189 Zurcher v. Stanford Daily, 436 U.S. 547, 559 (1978).

seems proper to vacate or remand the decision to address the issues that have emerged.

A. Proposed Methodologies

Several commentators have suggested approaches that seek to safeguard innocent parties' rights without compromising investigations. One such approach was advanced by Orin Kerr.[190] In his article, Kerr proposes an "exposure-based" approach that would distinguish between physical and virtual searches but adopts many of the traditional ideas of physical searches.[191] While remaining open for evolution, the approach would limit or abandon the plain view doctrine[192] and eliminate ex ante warrant limitations on the search processes.[193] This acknowledges that computer searches are as much an art as a science and that the parties involved are not sophisticated enough to lay out a search protocol beforehand.[194]

Alternatively, in direct response to the first *CDT* decision, Derek Regensburger advocated a different approach than the one advanced by Kerr.[195] In his solution, Regensburger suggested that existing law should be made easily modifiable to accommodate the recent development of computers and ESI.[196] To add sufficient protections, the approach requires that warrant requests to search ESI be based on specific assertions of necessity and not on vague or tangential relations to investigation.[197] Once a warrant is obtained under this higher scrutiny, any storage media seized could be searched extensively, founded partially on the idea that there is no expectation

190 *See* Kerr, *supra* note 137.

191 *Id.* at 584–85.

192 *Id.* at 566 ("Narrowing or even eliminating the plain view exception may eventually be needed to ensure that warrants to search computers do not become the functional equivalent of general warrants.").

193 *Id.* at 571–72 ("The ex ante strategy . . . wrongly assumes that prosecutors and magistrate judges have the knowledge needed to articulate search strategies before the search begins. In truth, the forensics process is too contingent and unpredictable for judges to establish effective ex ante rules.").

194 *Id.* at 572.

195 Derek Regensburger, *Bytes, Balco, and Barry Bonds: An Exploration of the Law Concerning the Search and Seizure of Computer Files and an Analysis of the Ninth Circuit's Decision in* United States v. Comprehensive Drug Testing, Inc., 97 CRIM. L. & CRIMINOLOGY 1151 (2007).

196 *Id.* at 1202.

197 *Id.*

of privacy in criminal materials.[198] Off-site searches should be utilized as they are more convenient for all parties.[199] However, the approach also demands a different approach for searches of innocent third parties, such as businesses. Here, the specific method of how the intermingled data will be separated must be detailed in the warrant, thereby taking no more than is necessary and avoiding wholesale removal of business computers.[200] Like Kerr, Regensburger also expresses skepticism about the plain view exception and suggests that it be eliminated or curtailed for digital searches.[201]

B. Finding the Right Balance

Both of the approaches advocated by Kerr and Regensburger are brilliantly thought out and deserve close scrutiny by courts confronted with these issues, but they each go too far in their limitations on the plain view doctrine. Plain view has been a recognized exception for decades[202] and is a crucial device in many investigations.[203] Aside from the issues with the Ninth Circuit's choosing to ignore the established doctrine,[204] plain view provides an efficient and minimally invasive method to find inculpatory evidence. Rather than requiring a waiver of plain view, courts should require that any evidence found in plain view during an ESI search be presented to the court via sworn affidavit by the examiner. This would ensure that the initial search did not serve as mere pretext and that the material was reached in compliance with the exception's requirements.[205]

198 *Id.* at 1203.

199 *Id.* at 1204.

200 *Id.* at 1205.

201 *Id.* at 1207.

202 *See generally* Coolidge v. New Hampshire, 403 U.S. 443 (1971) (holding a plain view seizure did not violate the defendant's Fourth Amendment rights).

203 *See, e.g.*, United States v. Wong, 334 F.3d 831 (9th Cir. 2003) (holding that child pornography found on a computer during a homicide investigation was in plain view).

204 *See supra* Part III.C.

205 *See generally* Andrew Vahid Moshirnia, *Separating Hard Fact from Hard Drive: A Solution for Plain View Doctrine in the Digital Domain*, 23 HARV. J.L. & TECH. 609 (2010) (advocating for a balancing of society's interests in public safety against the target's justified expectation of privacy to determine if plain view is justified). The approach put forth by Moshirnia is attractive in the example of *CDT* because it places the primary focus on the two actors the court seemed least concerned with in *CDT*: the target

It is also important that any approach to ESI searches have enough built-in flexibility to allow case agents to effectively communicate with computer personnel in order to facilitate an investigation. This would enable seemingly innocuous but relevant data to be found much more easily. To do this, the author proposes the "above and beyond" test. This would shift the burden of proving compliance to the government when the following questions are answered in the affirmative:

(1) Is the seized information related to the information sought in the warrant?

(2) Is there reason to suspect that the warrant served as pretext?

(3) Is the information above and beyond the warranted investigation such that the government significantly benefits from its discovery?

This test would determine whether the nontargeted information was reached only as a result of pretext or was genuinely found innocently. To do this, the court would review the seizure and decide whether the found information was within the context of the initial investigation. If the area searched is related to the warrant but reveals additional information that is above and beyond the warrant but is also related to the investigation, the government should have to prove it came upon that information innocently. This determination would consider file structure, the party's culpability, the approved scope of the warrant, and any other relevant factors.

In a case like *CDT*, the file structure was easily determined, the party was not inculpated in any way, the warrant was specifically tailored to reveal relevant information, and, perhaps most importantly, the information had already been sought in previous warrants. Accordingly, there should be a strong presumption that the additional incriminating materials were above and beyond the authorization of the warrant. The government's actions should have been seen, as they were by the court, as egregious and against the "spirit" of the warrant. That is, the data taken were easily seen as the result of pretext and should be suppressed. However, if the case agent had somehow stumbled upon evidence of fraud or illegal narcotic trafficking, this would be well outside the perceived goal of the investigation and not just above and beyond the warrant; therefore, it

and society. By avoiding a test that critiques government action directly, reckless searches are unlikely to be stymied.

should be allowed to support further prosecution. To suppress such evidence that is obtained under established exceptions to the Fourth Amendment seems overly burdensome.

Although it could be argued that this is similar to the subjective inadvertence test, which has been rejected, it is more akin to other Fourth Amendment doctrines that ask whether an officer's actions were objectively reasonable in light of the circumstances. The Supreme Court has declined to examine an agent's subjective intent and instead has focused on whether the circumstances, viewed objectively, justified the agent's conduct.[206]

CONCLUSION

The Ninth Circuit made some sweeping changes with the *CDT* decision, and the ramifications are still largely unknown. However, the guidelines have certainly proved difficult, if not impossible, to follow. Currently, the case is awaiting decision by the Ninth Circuit as to whether a full-court en banc rehearing should be held. In the author's view, this could only help both sides in the controversy: the government would get a legitimate opportunity to brief the issues not originally presented on appeal, and the court would get a chance to clarify some seemingly untenable positions. In the meantime, prosecutors and magistrate judges are scrambling to find the contours of the guidelines. Until those contours are determined, investigations will continue to be hampered by the current state of the law.

ADDENDUM

On September 13, 2010, the Ninth Circuit filed a per curiam opinion in the *CDT* case.[207] In the opinion, the guidelines that were previously a part of the majority opinion penned by Chief Judge Kozinski have been relegated to a concurrence.[208]

In his concurrence, which is joined by four other members of the eleven-judge panel, Judge Kozinski frames the guidelines as offering

---

[206] *See, e.g.*, Brigham City v. Stuart, 547 U.S. 398, 404 (2006) ("An action is 'reasonable' under the Fourth Amendment, regardless of the individual officer's state of mind, as long as the circumstances, viewed objectively, justify the action.") (internal quotation marks omitted).

[207] United States v. Comprehensive Drug Testing, Inc., Nos. 05-10067, 05-15006, 05-55354, 2010 WL 3529247 (9th Cir. Sept. 13, 2010).

[208] *Id.* at *16.

"the government a safe harbor, while protecting the people's right to privacy and property in their papers and effects."[209] He goes on to say that "heeding this guidance will significantly increase the likelihood that the searches and seizures of electronic storage that [district and magistrate judges] authorize will be deemed reasonable and lawful."[210] The language used in defining the guidelines themselves is identical to that of the original opinion, and no effort is made to explain the new location beyond a claim that it is merely a restatement of current law.[211]

The effect of the per curiam opinion is clear: the *CDT* guidelines are not binding on warrants authorizing ESI searches. However, given the number of judges who joined in Kozinski's concurrence and the stern recommendation that the guidance be followed in the future, it is likely that future ESI searches will still be subjected to the *CDT* guidelines in principle if not in fact.

Practically, the Ninth Circuit has protected the *CDT* guidelines. By placing them in a concurrence, and thereby not binding lower courts to their application, the court makes the issue moot on appeal. The per curiam opinion fixes the major flaw in the original *CDT* decision, which was the overreaching represented by the guidelines. Thus, the government is unlikely to seek certiorari with the Supreme Court. Even if certiorari were sought, the Supreme Court would be unlikely to grant it given the rather simple conclusion that the search was improper under current Fourth Amendment doctrine. Without the guidelines to take issue with, there is simply nothing to be gained on appeal.

The *CDT* drama is now likely to conclude. In the end, the *CDT* guidelines will likely become another signpost in the journey to a coherent and fair application of the Fourth Amendment to ESI searches.

---

209 *Id.* at *14.

210 *Id.*

211 *Id.* at *16 ("This guidance is hardly revolutionary. It's essentially *Tamura*'s solution to the problem of necessary over-seizing of evidence."). Cynically, the prospect of a full panel en banc review likely motivated the court to reissue the opinion in its new form.