

H

United States Court of Appeals,
Ninth Circuit.
UNITED STATES of America, Plaintiff-Appellant,
v.
COMPREHENSIVE DRUG TESTING, INC., Defendant-Appellee.
Major League Baseball Players Association, Petitioner-Appellee,
v.
United States of America, Respondent-Appellant.
In re Seal 1, Plaintiff-Appellant,
v.
Seal 2, Defendant-Appellee.
Nos. 05-10067, 05-15006, 05-55354.

Argued and Submitted Dec. 18, 2008.
Filed Sept. 13, 2010.

Before [ALEX KOZINSKI](#), Chief Judge, [ANDREW J. KLEINFELD](#), [SUSAN P. GRABER](#), [KIM McLANE WARDLAW](#), [W. FLETCHER](#), [RICHARD A. PAEZ](#), [MARSHA S. BERZON](#), [CONSUELO M. CALLAHAN](#), [CARLOS T. BEA](#), [MILAN D. SMITH, JR.](#) and [SANDRA S. IKUTA](#), Circuit Judges.

OPINION

This case is about a federal investigation into steroid use by professional baseball players. More generally, however, it's about the procedures and safeguards that federal courts must observe in issuing and administering search warrants and subpoenas for electronically stored information.

Facts

The complex facts underlying this case are well summed up in the panel's opinion and dissent, and we refer the interested reader there for additional information. [United States v. Comprehensive Drug Testing, Inc., 513 F.3d 1085 \(9th Cir.2008\)](#). We reiterate here only the key facts.

In 2002, the federal government commenced an investigation into the Bay Area Lab Cooperative (Balco), which it suspected of providing steroids to professional baseball players. That year, the Major League Baseball Players Association (the Players) also entered into a collective bargaining agreement with Major League Baseball providing for suspicionless drug testing of all players. Urine samples were to be collected during the first year of the agreement and each sample was to be tested for banned substances. The players were assured that the results would remain anonymous and confidential; the purpose of the testing was solely to determine whether more than five percent of players tested positive, in which case there would be additional testing in future seasons.

Comprehensive Drug Testing, Inc. (CDT), an independent business, administered the program and collected the specimens from the players; the actual tests were performed by Quest Diagnostics, Inc., a laboratory. CDT maintained the list of players and their respective test results; Quest kept the actual specimens

on which the tests were conducted.

During the Balco investigation, federal authorities learned of ten players who had tested positive in the CDT program. The government secured a grand jury subpoena in the Northern District of California seeking *all* “drug testing records and specimens” pertaining to Major League Baseball in CDT’s possession. CDT and the Players tried to negotiate a compliance agreement with the government but, when negotiations failed, moved to quash the subpoena.

The day that the motion to quash was filed, the government obtained a warrant in the Central District of California authorizing the search of CDT’s facilities in Long Beach. Unlike the subpoena, the warrant was limited to the records of the ten players as to whom the government had probable cause. When the warrant was executed, however, the government seized and promptly reviewed the drug testing records for hundreds of players in Major League Baseball (and a great many other people).

The government also obtained a warrant from the District of Nevada for the urine samples on which the drug tests had been performed. These were kept at Quest’s facilities in Las Vegas. Subsequently, the government obtained additional warrants for records at CDT’s facilities in Long Beach and Quest’s lab in Las Vegas. Finally, the government served CDT and Quest with new subpoenas in the Northern District of California, demanding production of the same records it had just seized.

*2 CDT and the Players moved in the Central District of California, pursuant to [Federal Rule of Criminal Procedure 41\(g\)](#), for return of the property seized there. Judge Cooper found that the government had failed to comply with the procedures specified in the warrant and, on that basis and others, ordered the property returned. We will refer to this as the Cooper Order.

CDT and the Players subsequently moved in the District of Nevada, pursuant to [Federal Rule of Criminal Procedure 41\(g\)](#), for return of the property seized under the warrants issued by that court. The matter came before Judge Mahan, who granted the motion and ordered the government to return the property it had seized, with the exception of materials pertaining to the ten identified baseball players. We will refer to this as the Mahan Order.

CDT and the Players finally moved in the Northern District of California, pursuant to [Federal Rule of Criminal Procedure 17\(c\)](#), to quash the latest round of subpoenas and the matter was heard by Judge Illston. (The original subpoena, and the motion to quash it that was filed in 2003, aren’t before us.) In an oral ruling, Judge Illston quashed the subpoenas. We will refer to this as the Illston Quashal. *See* Bryan A. Garner, *A Dictionary of Modern American Legal Usage* 725 (2d ed.1995).

All three judges below expressed grave dissatisfaction with the government’s handling of the investigation, some going so far as to accuse the government of manipulation and misrepresentation. The government nevertheless appealed all three orders and a divided panel of our court reversed the Mahan Order and the Illston Quashal, but (unanimously) found that the appeal from the Cooper Order was untimely. Upon a vote of eligible judges, we took the case en banc. As luck would have it, none of the three judges on the original panel was drawn for this

en banc court. Nevertheless, we rely heavily on their work in resolving the case now before us.

Discussion

For reasons that will become apparent, we don't consider the three orders chronologically. Rather, we consider the Cooper Order first, the Mahan Order next and the Illston Quashal last.

1. The Cooper Order

The three-judge panel unanimously held that the government's appeal from the Cooper Order was untimely. [Comprehensive Drug Testing, 513 F.3d at 1096-1101, 1128](#). We agree with the panel and adopt its analysis of the issue, seeing no reason to burden the pages of the Federal Reporter by redoing the work the panel already performed so well. On that basis, we dismiss the government's appeal in No. 05-55354.

This does not end our discussion of the Cooper Order, however, because it has substantial consequences for the remaining two cases before us. As Judge Thomas pointed out in his panel dissent, once the Cooper Order became final, the government became bound by the factual determinations and issues resolved against it in that order. [Comprehensive Drug Testing, 513 F.3d at 1130](#). Specifically, Judge Cooper found that the government failed to comply with the conditions of the warrant designed to segregate information as to which the government had probable cause from that which was swept up only because the government didn't have the time or facilities to segregate it at the time and place of the seizure. Cooper Order at 4. Relatedly, Judge Cooper determined that the government failed to comply with the procedures outlined in our venerable precedent, [United States v. Tamura, 694 F.2d 591 \(9th Cir.1982\)](#), which are designed to serve much the same purpose as the procedures outlined in the warrant. Finally, Judge Cooper concluded that the government's actions displayed a callous disregard for the rights of third parties, viz., those players as to whom the government did not already have probable cause and who could suffer dire personal and professional consequences from a disclosure of their test results.

*3 The affidavit supporting the first search warrant, the one that sought the drug testing records of the ten suspected baseball players, contains an extensive introduction that precedes any information specific to this case. The introduction seeks to justify a broad seizure of computer records from CDT by explaining the generic hazards of retrieving data that are stored electronically. 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 (pes-to.recipe in lieu of blackmail.photos) or a false extension (.doc in lieu of .jpg or .gz). In addition, the data might be erased or hidden; there might be booby traps that “destroy or alter data if certain procedures are not scrupulously followed,” Warrant Affidavit at 3; certain files and programs might not be accessible at all without the proper software, which may not be available on the computer that is being searched; there may simply be too much information to be examined at the site; or data might be encrypted or compressed, requiring passwords, key-cards or other external devices to retrieve. *Id.* at 4. 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 evi-

dence.”

By reciting these hazards, the government made a strong case for off-site examination and segregation of the evidence seized. The government sought the authority to seize considerably more data than that for which it had probable cause, including various computers or computer hard drives and related storage media, and to have the information examined and segregated in a “controlled environment, such as a law enforcement laboratory.” While the government did not point to any specific dangers associated with CDT, which is after all a legitimate business not suspected of any wrongdoing, it nevertheless made a strong generic case that the data in question could not be thoroughly examined or segregated on the spot.

Not surprisingly, the magistrate judge was persuaded by this showing and granted broad authority for seizure of data, including the right to remove pretty much any computer equipment found at CDT's Long Beach facility, along with any data storage devices, manuals, logs or related materials. The warrant also authorized government agents to examine all the data contained in the computer equipment and storage devices, and to attempt to recover or restore hidden or erased data. The magistrate judge, however, wisely made such broad seizure subject to certain procedural safeguards, roughly based on our *Tamura* opinion. Thus, the government was first required to examine the computer equipment and storage devices at CDT to determine whether information pertaining to the ten identified players “c[ould] be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve the data.”

*4 The warrant also contained significant restrictions on how the seized data were to be handled. These procedures were designed to ensure that data beyond the scope of the warrant would not fall into the hands of the investigating agents. Thus, the initial review and segregation of the data was not to be conducted by the investigating case agents but by “law enforcement personnel trained in searching and seizing computer data (‘computer personnel’),” whose job it would be to determine whether the data could be segregated on-site. These computer personnel-not the case agents-were specifically authorized to examine all the data on location to determine how much had to be seized to ensure the integrity of the search. Moreover, if the computer personnel determined that the data did not “fall within any of the items to be seized pursuant to this warrant or is not otherwise legally seized,” the government was to return those items “within a reasonable period of time not to exceed 60 days from the date of the seizure unless further authorization [was] obtained from the Court.” Subject to these representations and assurances, Magistrate Judge Johnson authorized the seizure.

A word about *Tamura* is in order, and this seems as good a place as any for it. *Tamura*, decided in 1982, just preceded the dawn of the information age, and all of the records there were on paper. The government was authorized to seize evidence of certain payments received by Tamura from among the records of Marubeni, his employer. To identify the materials pertaining to the payments involved a three step procedure: Examining computer printouts to identify a transaction; locating the voucher that pertained to that payment; and finding the check that corresponded to the voucher. [*Tamura*, 694 F.2d at 594-95](#). The government agents soon realized that this process would take a long time unless they got help from the Marubeni employees who were present. The employees,

however, steadfastly refused, so the agents seized several boxes and dozens of file drawers to be sorted out in their offices at their leisure.

We disapproved the wholesale seizure of the documents and particularly the government's failure to return the materials that were not the object of the search once they had been segregated. *Id.* at 596-97. However, we saw no reason to suppress the properly seized materials just because the government had taken more than authorized by the warrant. For the future, though, we suggested that “[i]n the comparatively rare instances where documents are so intermingled that they cannot feasibly be sorted on site, ... the Government [should] seal[] and hold[] the documents pending approval by a magistrate of a further search, in accordance with the procedures set forth in the American Law Institute's Model Code of Pre-Arrest Procedure.” *Id.* at 595-96. “If the need for transporting the documents is known to the officers prior to the search,” we continued, “they may apply for specific authorization for large-scale removal of material, which should be granted by the magistrate issuing the warrant only where on-site sorting is infeasible and no other practical alternative exists.” *Id.* at 596.

*5 No doubt in response to this suggestion in *Tamura*, the government here did seek advance authorization for sorting and segregating the seized materials off-site. But, as Judge Cooper found, “[o]nce the items were seized, the requirement of the Warrant that any seized items not covered by the warrant be first screened and segregated by computer personnel was completely ignored .” Brushing aside an offer by on-site CDT personnel to provide all information pertaining to the ten identified baseball players, the government copied from CDT's computer what the parties have called the “Tracey Directory” which contained, in Judge Cooper's words, “information and test results involving hundreds of other baseball players and athletes engaged in other professional sports.”

Counsel for CDT, contacted by phone, pleaded in vain that “all material not pertaining to the specific items listed in the warrant be reviewed and redacted by a Magistrate or Special Master before it was seen by the Government.” Instead, the case agent “himself reviewed the seized computer data and used what he learned to obtain the subsequent search warrants issued in Northern California, Southern California, and Nevada.” Judge Cooper also found that, in conducting the seizure in the manner it did, “[t]he Government demonstrated a callous disregard for the rights of those persons whose records were seized and searched outside the warrant.”

As previously noted, the government failed to timely appeal the Cooper Order and is therefore bound by its factual determinations and legal rulings. The government also failed to appeal another ruling, by Judge Illston, that ordered return of the Tracey directory and all copies thereof. We will call this the Illston Order. It held unlawful the government's failure to segregate data covered by the warrant from data not covered by it simply because both types were intermingled in the Tracey directory. In reaching this conclusion, Judge Illston necessarily rejected the argument about the scope of the warrant the government made before Judge Mahan. The Illston Order therefore has preclusive effect on the core legal questions resolved in the Mahan Order, viz., the government's failure to segregate intermingled data, as required by *Tamura*.

* * *

2. The Mahan Order

*6 [2] Like Judges Cooper and Illston, Judge Mahan determined that “[t]he government callously disregarded the affected players’ constitutional rights.” Judge Mahan also concluded that the government “unreasonab[ly] ... refuse[d] to follow the procedures set forth in *United States v. Tamura* ... upon learning that drug-testing records for the ten athletes named in the original April 8 warrants executed at Quest and at [CDT] were intermingled with records for other athletes not named in those warrants.” We can and do uphold these findings based on the preclusive effect of the Cooper and Illston Orders. However, because the matter is important, and to avoid any quibble about the proper scope of preclusion, we also dispose of the government’s contrary arguments.

* * *

B. Initial Review by Computer Personnel

*7 The government also failed to comply with another important procedure specified in the warrant, namely that “computer personnel” conduct the initial review of the seized data and segregate materials not the object of the warrant for return to their owner. As noted, Judge Cooper found that these procedures were completely ignored; rather, the case agent immediately rooted out information pertaining to *all* professional baseball players and used it to generate additional warrants and subpoenas to advance the investigation. Judge Illston found the same. The record reflects no forensic lab analysis, no defusing of booby traps, no decryption, no cracking of passwords and certainly no effort by a dedicated computer specialist to separate data for which the government had probable cause from everything else in the Tracey Directory. Instead, as soon as the Tracey Directory was extracted from the CDT computers, the case agent assumed control over it, examined the list of all professional baseball players and extracted the names of those who had tested positive for steroids. *See Comprehensive Drug Testing*, 513 F.3d at 1134-35 (Thomas, J., dissenting). Indeed, the government admitted at the hearing before Judge Mahan that “the idea behind taking [the copy of the Tracey Directory] was to take it and later on briefly peruse it to see if there was anything above and beyond that which was authorized for seizure in the initial warrant.” The government agents obviously were counting on the search to bring constitutionally protected data into the plain view of the investigating agents.

But it was wholly unnecessary for the case agent to view any data for which the government did not already have probable cause because there was an agent at the scene who was specially trained in computer forensics. This agent did make an initial determination that the CDT computer containing the Tracey Directory could not be searched and segregated on-site, and that it would be safe to copy the Tracey Directory, rather than seizing the entire hard drive or computer. After that copy was made, however, it was turned over to the case agent, and the specialist did nothing further to segregate the target data from that which was swept up simply because it was nearby or commingled. The sequence of events supports the suspicion that representations in the warrant about the necessity for broad authority to seize materials were designed to give the government access to the full list of professional baseball players and their confidential drug testing records.

The government argues that it didn’t violate the warrant protocol because the

warrant didn't specify that *only* computer personnel could examine the seized files, and the case agent was therefore entitled to view them alongside the computer specialist. This, once again, is sophistry. It would make no sense to represent that computer personnel would be used to segregate data if investigatory personnel were also going to access all the data seized. What would be the point? The government doesn't need instruction from the court as to what kind of employees to use to serve its own purposes; the representation in the warrant that computer personnel would be used to examine and segregate the data was obviously designed to reassure the issuing magistrate that the government wouldn't sweep up large quantities of data in the hope of dredging up information it could not otherwise lawfully seize. Judge Cooper found that the government utterly failed to follow the warrant's protocol. Judge Illston also found that the government's seizure, in callous disregard of the Fourth Amendment, reached information clearly not covered by a warrant. These findings are binding on the government, but simple common sense leads to precisely the same conclusion: This was an obvious case of deliberate overreaching by the government in an effort to seize data as to which it lacked probable cause.

C. Federal Rule of Criminal Procedure 41(g)

*8 [3] Judge Mahan cured this overreaching by ordering the government to return the illegally seized data. We have long held that [Rule 41\(g\)](#) empowers district courts to do just that. [Ramsden v. United States, 2 F.3d 322 \(9th Cir.1993\)](#). Though styled as a motion under a Federal Rule of Criminal Procedure, when the motion is made by a party against whom no criminal charges have been brought, such a motion is in fact a petition that the district court invoke its civil equitable jurisdiction. [Id. at 324](#). We agree with the panel that the district court in this case did not abuse its discretion in choosing to exercise that jurisdiction. [Comprehensive Drug Testing, 513 F.3d at 1104](#).

* * *

[10][11] We affirm Judge Mahan on an alternative ground as well: When, as here, the government comes into possession of evidence by circumventing or willfully disregarding limitations in a search warrant, it must not be allowed to benefit from its own wrongdoing by retaining the wrongfully obtained evidence or any fruits thereof. When the district court determines that the government has obtained the evidence through intentional wrongdoing-rather than through a technical or good faith mistake-it should order return of the property without the need for balancing that is applicable in the more ordinary case.

Concluding Thoughts

This case well illustrates both the challenges faced by modern law enforcement in retrieving information it needs to pursue and prosecute wrongdoers, and the threat to the privacy of innocent parties from a vigorous criminal investigation. At the time of *Tamura*, most individuals and enterprises kept records in their file cabinets or similar physical facilities. Today, the same kind of data is usually stored electronically, often far from the premises. Electronic storage facilities intermingle data, making them difficult to retrieve without a thorough understanding of the filing and classification systems used-something that can often only be determined by closely analyzing the data in a controlled environment. *Tamura* involved a few dozen boxes and was considered a broad seizure; but

even inexpensive electronic storage media today can store the equivalent of millions of pages of information.

***12** Wrongdoers and their collaborators have obvious incentives to make data difficult to find, but parties involved in lawful activities may also encrypt or compress data for entirely legitimate reasons: protection of privacy, preservation of privileged communications, warding off industrial espionage or preventing general mischief such as identity theft. Law enforcement today thus has a far more difficult, exacting and sensitive task in pursuing evidence of criminal activities than even in the relatively recent past. The legitimate need to scoop up large quantities of data, and sift through it carefully for concealed or disguised pieces of evidence, is one we've often recognized. See, e.g., [United States v. Hill, 459 F.3d 966 \(9th Cir.2006\)](#).

This pressing need of law enforcement for broad authorization to examine electronic records, so persuasively demonstrated in the introduction to the original warrant in this case, see pp. 13944-45 *supra*, creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant. The problem can be stated very simply: There is no way to be sure exactly what an electronic file contains without somehow examining its contents—either by opening it and looking, using specialized forensic software, keyword searching or some other such technique. But electronic files are generally found on media that also contain thousands or millions of other files among which the sought-after data may be stored or concealed. By necessity, government efforts to locate particular files will require examining a great many other files to exclude the possibility that the sought-after data are concealed there.

Once a file is examined, however, the government may claim (as it did in this case) that its contents are in plain view and, if incriminating, the government can keep it. Authorization to search *some* computer files therefore automatically becomes authorization to search all files in the same sub-directory, and all files in an enveloping directory, a neighboring hard drive, a nearby computer or nearby storage media. Where computers are not near each other, but are connected electronically, the original search might justify examining files in computers many miles away, on a theory that incriminating electronic data could have been shuttled and concealed there.

The advent of fast, cheap networking has made it possible to store information at remote third-party locations, where it is intermingled with that of other users. For example, many people no longer keep their email primarily on their personal computer, and instead use a web-based email provider, which stores their messages along with billions of messages from and to millions of other people. Similar services exist for photographs, slide shows, computer code and many other types of data. As a result, people now have personal data that are stored with that of innumerable strangers. Seizure of, for example, Google's email servers to look for a few incriminating messages could jeopardize the privacy of millions.

***13** It's no answer to suggest, as did the majority of the three-judge panel, that people can avoid these hazards by not storing their data electronically. To begin with, the choice about how information is stored is often made by someone other than the individuals whose privacy would be invaded by the search. Most people have no idea whether their doctor, lawyer or accountant maintains records in

paper or electronic format, whether they are stored on the premises or on a server farm in Rancho Cucamonga, whether they are commingled with those of many other professionals or kept entirely separate. Here, for example, the Tracey Directory contained a huge number of drug testing records, not only of the ten players for whom the government had probable cause but hundreds of other professional baseball players, thirteen other sports organizations, three unrelated sporting competitions, and a non-sports business entity-thousands of files in all, reflecting the test results of an unknown number of people, most having no relationship to professional baseball except that they had the bad luck of having their test results stored on the same computer as the baseball players.

Second, there are very important benefits to storing data electronically. Being able to back up the data and avoid the loss by fire, flood or earthquake is one of them. Ease of access from remote locations while traveling is another. The ability to swiftly share the data among professionals, such as sending MRIs for examination by a [cancer](#) specialist half-way around the world, can mean the difference between death and a full recovery. Electronic storage and transmission of data is no longer a peculiarity or a luxury of the very rich; it's a way of life. Government intrusions into large private databases thus have the potential to expose exceedingly sensitive information about countless individuals not implicated in any criminal activity, who might not even know that the information about them has been seized and thus can do nothing to protect their privacy.

It is not surprising, then, that all three of the district judges below were severely troubled by the government's conduct in this case. Judge Mahan, for example, asked "what ever happened to the Fourth Amendment? Was it ... repealed somehow?" Judge Cooper referred to "the image of quickly and skillfully moving the cup so no one can find the pea." And Judge Illston regarded the government's tactics as "unreasonable" and found that they constituted "harassment." Judge Thomas, too, in his panel dissent, expressed frustration with the government's conduct and position, calling it a "breathtaking expansion of the 'plain view' doctrine, which clearly has no application to intermingled private electronic data." [Comprehensive Drug Testing, 513 F.3d at 1117.](#)

Everyone'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. *Tamura* has provided a workable framework for almost three decades, and might well have sufficed in this case had its teachings been followed. We have updated *Tamura* to apply to the daunting realities of electronic searches.

*14 [\[18\]](#) We recognize the reality that over-seizing is an inherent part of the electronic search process and proceed on the assumption that, when it comes to the seizure of electronic records, this will be far more common than in the days of paper records. This calls for greater vigilance on the part of judicial officers in striking 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 process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect.

* * *

The judgments in Nos. 05-15006 (the Mahan Order) and 05-10067 (the Illston Quashal) are affirmed.

Chief Judge [KOZINSKI](#), with whom Judges [KLEINFELD](#), [W. FLETCHER](#), [PAEZ](#) and [M. SMITH](#) join, concurring:

The opinion correctly disposes of the Fourth Amendment issues in this case, so I join it in full. I write separately because these issues are important and likely often to arise again. It would therefore be useful to provide guidance about how to deal with searches of electronically stored data in the future so that the public, the government and the courts of our circuit can be confident such searches and seizures are conducted lawfully. The guidance below offers the government a safe harbor, while protecting the people's right to privacy and property in their papers and effects. District and magistrate judges must exercise their independent judgment in every case, but heeding this guidance will significantly increase the likelihood that the searches and seizures of electronic storage that they authorize will be deemed reasonable and lawful.

* * *

When the government wishes to obtain a warrant to examine a computer hard drive or electronic storage medium to search for certain incriminating files, or when a search for evidence could result in the seizure of a computer, *see, e.g., United States v. Giberson*, [527 F.3d 882 \(9th Cir.2008\)](#), magistrate judges should insist that the government forswear reliance on the plain view doctrine. They should also require the government to forswear reliance on any similar doctrine that would allow retention of data obtained only because the government was required to segregate seizable from non-seizable data. This will ensure that future searches of electronic records do not “make a mockery of *Tamura*”-indeed, the Fourth Amendment-by turning all warrants for digital data into general warrants. Maj. op. at 13950. If the government doesn't consent to such a waiver, the magistrate judge should order that the seizable and non-seizable data be separated by an independent third party under the supervision of the court, or deny the warrant altogether.

In addition, while it's perfectly appropriate for a warrant application to acquaint the issuing judicial officer with the theoretical risks of concealment and destruction of evidence, the government should also fairly disclose the *actual* degree of such risks in the case presented to the judicial officer. In this case, for example, the warrant application presented to Judge Johnson discussed the numerous theoretical risks that the data might be destroyed, but failed to mention that Comprehensive Drug Testing had agreed to keep the data intact until its motion to quash the subpoena could be ruled on by the Northern California district court, and that the United States Attorney's Office had accepted this representation. This omission created the false impression that, unless the data were seized at once, it would be lost. [Comprehensive Drug Testing](#), [513 F.3d at 1132](#) (Thomas, J., dissenting). Such pledges of data retention are obviously highly relevant in determining whether a warrant is needed at all and, if so, what its scope should be. If the government believes such pledges to be unreliable, it may say so and explain why. But omitting such highly relevant information altogether is inconsistent with the government's duty of candor in presenting a warrant appli-

cation. A lack of candor in this or any other aspect of the warrant application must bear heavily against the government in the calculus of any subsequent motion to return or suppress the seized data.

***15** The process of sorting, segregating, decoding and otherwise separating seizable data (as defined by the warrant) from all other data should also be designed to achieve that purpose and that purpose only. Thus, if the government is allowed to seize information pertaining to ten names, the search protocol should be designed to discover data pertaining to those names only, not to others, and not those pertaining to other illegality. For example, the government has sophisticated hashing tools at its disposal that allow the identification of well-known illegal files (such as child pornography) without actually opening the files themselves. These and similar search tools should not be used without specific authorization in the warrant, and such permission should only be given if there is probable cause to believe that such files can be found on the electronic medium to be seized.

To that end, the warrant application should normally include, or the issuing judicial officer should insert, a protocol for preventing agents involved in the investigation from examining or retaining any data other than that for which probable cause is shown. The procedure might involve, as in this case, a requirement that the segregation be done by specially trained computer personnel who are not involved in the investigation. In that case, it should be made clear that *only* those personnel may examine and segregate the data. The government should also agree that such computer personnel will not communicate any information they learn during the segregation process absent further approval of the court.

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. In a case such as this one, where the party subject to the warrant is not suspected of any crime, and where the privacy interests of numerous other parties who are not under suspicion of criminal wrongdoing are implicated by the search, the presumption should be that the segregation of the data will be conducted by an independent third party selected by the court. That third party should be prohibited from communicating any information learned during the search other than that covered by the warrant.

Once the data has been segregated (and, if necessary, redacted), the government agents involved in the investigation should be allowed to examine only the information covered by the terms of the warrant. Absent further judicial authorization, any remaining copies should be destroyed or, at least so long as they may be lawfully possessed by the party from whom they were seized, returned along with the actual physical medium that may have been seized (such as a hard drive or computer). The government should not retain copies of such returned data unless it obtains specific judicial authorization to do so.

***16** Also, within a time specified in the warrant, which should be as soon as practicable, the government should provide the issuing officer with a return disclosing precisely what it has obtained as a consequence of the search, and what it has returned to the party from whom it was seized. The return should include a sworn certificate that the government has destroyed or returned all copies of data that it's not entitled to keep. If the government believes it's entitled to retain data

as to which no probable cause was shown in the original warrant, it may seek a new warrant or justify the warrantless seizure by some means other than plain view.

This guidance can be summed up as follows:

1. Magistrate judges should insist that the government waive reliance upon the plain view doctrine in digital evidence cases. Pp. 13962-63 *supra*; *see maj. op.* at 13949-50.
2. Segregation and redaction of electronic data must be done either by specialized personnel or an independent third party. Pp. 13964-65 *supra*; *see maj. op.* at 13945-48, 13950-52. If the segregation is to be done by government computer personnel, the government must agree in the warrant application that the computer personnel will not disclose to the investigators any information other than that which is the target of the warrant.
3. Warrants and subpoenas must disclose the actual risks of destruction of information as well as prior efforts to seize that information in other judicial fora. Pp. 13963-64 *supra*; *see maj. op.* at 13944-45, 13957-58.
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. Pp. 13964-65 *supra*; *see maj. op.* at 13950-52.
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. P. 13965 *supra*; *see maj. op.* at 13952-56.

* * *

This guidance is hardly revolutionary. It's essentially *Tamura's* solution to the problem of necessary over-seizing of evidence. Just as *Tamura* has served as a guidepost for decades, the procedures outlined above should prove a useful tool for the future. Nothing any appellate court could say, however, would substitute for the sound judgment that magistrate judges must, and I am confident will, exercise in striking this delicate balance.

[CALLAHAN](#), Circuit Judge, with whom [IKUTA](#), Circuit Judge, joins, concurring in part and dissenting in part from the en banc panel's per curiam opinion:

I initially express my concerns with the proposed guidelines for searches of electronically stored data that are set forth in the Chief Judge's concurring opinion. The concurrence is not joined by a majority of the en banc panel and accordingly the suggested guidelines are not Ninth Circuit law. Nonetheless, although they are only suggestions, there are sound reasons for declining to follow them. In Section B of this dissent, I reiterate my objections to the majority's opinion as set forth in my concurring and dissenting opinion to Chief Judge Kozinski's initial opinion for the majority of the en banc panel. [United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989 \(9th Cir.2009\)](#) (en banc).

A.

As noted in my dissent from our initial en banc opinion, the breadth of the proposed guidelines for future digital evidence cases raises several serious concerns. Although I appreciate the desire to set forth a new framework with respect to searches of commingled electronic data, I remain wary of this prophylactic approach. The prescriptions go significantly beyond what is necessary to resolve this case.

Furthermore, the proffered “guidelines” are troubling because they are overbroad, unreasonably restrictive of how law enforcement personnel carry out their work, and unsupported by citations to legal authority. For example, the concurring opinion does not explain why it is now appropriate to grant heightened Fourth Amendment protections in the context of searches of computers based on the nature of the technology involved when we have previously cautioned just the opposite. See [United States v. Giberson, 527 F.3d 882, 887-88 \(9th Cir.2008\)](#) (declining to impose heightened Fourth Amendment protections in computer search cases as a result of a computer's ability to store large amounts of potentially intermingled information, and stating that such heightened protections must be “based on a principle that is not technology-specific”).

The concurring opinion also fails to acknowledge that its proffered guidance conflicts with the amendments to [Federal Rule of Criminal Procedure 41\(f\)\(1\)\(B\)](#), effective December 1, 2009. For instance, [Rule 41\(f\)\(1\)\(B\)](#) now states that in cases where an officer is seizing or copying electronically stored information, “[t]he officer may retain a copy of the electronically stored information that was seized or copied.” This provision directly contradicts the suggestion that “[t]he government should not retain copies of such returned data.” Conc. Op. at 13965. Similarly, [Rule 41\(f\)\(1\)\(B\)](#) now provides that “[i]n a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied.” The concurring opinion, however, suggests that “the government should provide the issuing officer with a return disclosing precisely what it has obtained as a consequence of the search, and what it has returned to the party from whom it was seized.” Conc. Op. at 13965. Presumably these suggestions are superseded by the detailed amendments to [Rule 41](#), which provide comprehensive guidance in this area.

*20 In addition, the suggested protocols essentially jettison the plain view doctrine in digital evidence cases, urging that magistrate judges “insist that the government waive reliance upon the plain view doctrine in digital evidence cases.” [FNI](#) Conc. Op. at 13963. This is put forth without explaining why the Supreme Court's case law or our case law dictates or even suggests that the plain view doctrine should be entirely abandoned in digital evidence cases. Instead of tailoring its analysis of the plain view doctrine to the facts of this case, the concurring opinion takes the bold, and unnecessary step of casting that doctrine aside. The more prudent course would be to allow the contours of the plain view doctrine to develop incrementally through the normal course of fact-based case adjudication. A measured approach based on the facts of a particular case is especially warranted in the case of computer-related technology, which is constantly and quickly evolving.

Moreover, the concurring opinion offers no legal authority for its proposal requiring the segregation of computer data by specialized personnel or an independent third party. *See* Conc. Op. at 13964-65, 13966. Also, the proposed *ex ante* restriction on law enforcement investigations raises practical, cost-related concerns. With respect to using an in-house computer specialist to segregate data, the suggestion essentially would require that law enforcement agencies keep a “walled-off,” non-investigatory computer specialist on staff for use in searches of digital evidence. To comply, 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. The alternative would be to use an independent third party consultant, which no doubt carries its own significant expense. Both of these options would force law enforcement agencies to incur great expense, perhaps a crushing expense for a smaller police department that already faces tremendous budget pressures.

In sum, although the suggestions are well-intentioned, they certainly are not legally compelled and their adoption would create more problems than it would solve. Certainly the Chief Judge and my colleagues who have joined his concurring opinion may express their opinions on future protocols; however, their suggestions should not be confused with the en banc court's opinion which, although I dissent from it, is properly confined to the issues required to decide the appeal.