May, 2007

Search and Seizure on Steroids: United States v. Comprehensive Drug Testing and Its Consequences for Private Information Stored on Commercial Electronic Databases

Aaron S Lowenstein

Search and Seizure on Steroids: *United States v. Comprehensive Drug Testing* and Its Consequences for Private Information Stored on Commercial Electronic Databases

Aaron Seiji Lowenstein
May 2007

ABSTRACT

This article critiques the Ninth Circuit's recent decision in United States v. Comprehensive Drug Testing. *This case received some attention because it stems from the investigation into the use of steroids in Major League Baseball. It should have received much more attention, however, because of its troubling expansion of the government's authority to access our private digital information without a warrant.*

Executing a search warrant for information stored on a computer database poses special problems. Because targets of government investigations can easily conceal incriminating digital evidence, investigators often must search an entire computer hard drive in order to effectively execute a search warrant. Yet such probing, comprehensive searches clash with the Fourth Amendment's particularity requirements. Constitutional concerns are amplified when the government conducts a comprehensive search for information contained on a commercial electronic database, which often will result in the exposure of private information relating to thousands of persons with no connection the investigation.

Such was the dilemma posed in United States v. Drug Testing. *This article assesses the impact of the court's decision on the privacy rights of individuals with personal information stored on commercial electronic databases and argues that the court wrongly balanced the governmental and private interests at stake. As a result, this decision has ominous consequences for protections against search and seizure in the digital age.*

I. Introduction

Details about innumerable aspects of our personal lives exist in a multitude of electronic databases that we do not control. Stored on the internal computer networks of schools, health care facilities, financial institutions, law firms, and insurance companies are catalogues of our medical, educational, financial, legal, and employment histories – usually intermingled with the histories of hundreds, or even thousands, of other persons. Often, we divulge to these outside entities private information – such as our medical problems or financial transactions – with the subjective belief that it will remain confidential. Of course we do so knowing that the government could theoretically compel the disclosure of our personal information. But most of us believe that this could only happen once the government obtained a warrant.

The recent Ninth Circuit decision of *United States v. Comprehensive Drug Testing*[1] (which happens to stem from the investigation into steroid use in Major League Baseball[2]), may challenge these beliefs. The decision in this case, if read most favorably for law enforcement, allows government agents to search and seize private information stored on a commercial electronic database without a warrant – without even particularized suspicion of criminal conduct – so long as someplace on the same database there is other information that is responsive to a search warrant. The government could seize one person's private information under these circumstances even if the information responsive to the search warrant pertains to a completely different and unrelated person. Furthermore, if one's private information happened to provide evidence of a new, previously unsuspected crime, the government would be free to use that evidence as a basis for seeking a further search warrant or for bringing criminal charges.

---

[1] 473 F.3d 915 (9th Cir. 2006).

[2] *See*, *e.g.*, Bob Egelko, *100 Big-Leaguers Steroid-Positive in 2003 Season – Court Rules Federal Prosecutors Can Use Tests for Investigation*, S.F. CHRONICLE, Dec. 28, 2006, at B1.

This article critiques *Comprehensive Drug Testing* in the context of the development of computer search and seizure law and assesses its impact on the privacy rights of individuals with personal data stored on commercial electronic databases.

The surprising outcomes in *Comprehensive Drug Testing* result from the court's poor answer to a vexing question: what rules should apply to the government's search of intermingled computer documents? Evidence – i.e. materials that are responsive to a search warrant – is said to be "intermingled" when it is so mixed with irrelevant materials that concerns of time and convenience prevent government agents from separating the wheat from the chaff at the location of the search. As a practical matter, potentially every search of a computer database presents a problem of intermingled documents. Computer users, particularly those who are targets of criminal investigations, may organize information on their computers in idiosyncratic and non-intuitive ways. Additionally, computers can store a tremendous quantity and variety of data. These characteristics make it difficult for government investigators to locate the evidence specified on a search warrant in a timely fashion. Thus, the government has argued on many occasions that its agents should have authorization to make a precise copy of the targeted computer hard drive and to conduct a thorough off-site search for the evidence specified on the warrant.

The trouble with this approach is that it would permit the seizure of large amounts of information for which the government has no independent authority to search. This is in tension with the fundamental Fourth Amendment principles that the government should not conduct searches under the authority of "general warrants"[3] and that all warrants should "particularly [describe] the place to be searched and the persons or things to be seized."[4] These constitutional concerns are heightened by the fact that government seizures of entire computer databases will usually be very intrusive, given

[3] *Payton v. New York*, 445 U.S. 573, 583 (1980).

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

that people tend to store on computers vast quantities and varieties of private information. These concerns are greater still when a search warrant specifies information stored on a commercial electronic database, like the ones at issue in *Comprehensive Drug Testing*. In such cases, the government's seizure would expose the private information of numerous persons with no connection to the underlying investigation.

In Part II.A., I explore some basic differences between physical searches and computer searches. These differences help explain many of the doctrinal moves that courts have made in their efforts to translate ancient search and seizure principles into a digital framework. In Part II.B., I survey the myriad ways in which courts have tackled the intermingled documents problem in the computer context. This overview flushes out some of the rules that courts have implemented in their efforts to reconcile the competing concerns at stake: allowing government agents to effectively execute search warrants for digital information and protecting against warrantless government seizures of data on computer storage systems. This provides a background for understanding the court's ruling in *Comprehensive Drug Testing*.

Part III contains a detailed summary of the *Comprehensive Drug Testing* decision and its lengthy and bitter dissent. Despite the majority's efforts to protect Fourth Amendment interests, the dissent persuasively argued that the ruling left gaping areas in which the government remained free to engage in an unfettered review of private electronic information without a warrant.

To better gauge the effect of this opinion, Part IV examines the extent to which independent constitutional, statutory, or common law principles might protect the privacy interests of individuals whose private digital information is seized on the theory that it is intermingled with evidence responsive to a search warrant. These principles would limit the government's ability to conduct broad searches only in limited circumstances. Additionally, defendants prosecuted on the basis of evidence that the

government obtained in violation of these principles would nevertheless lack a suppression remedy most of the time.

Thus, after *Comprehensive Drug Testing*, Fourth Amendment protections have taken a large step backward. Private information stored in commercial electronic databases is no longer covered by its protective shadow. There are various ways of restoring these protections, while simultaneously accommodating the government's need to effectively execute search warrants of commercial electronic databases. The surest way, however, is for other courts to backpedal from this decision. Given the ever-increasing importance of computers and large commercial electronic databases in our daily lives, they had better hurry.

II. The Search and Seizure of Evidence in Computer Storage

The principles of search and seizure have for the most part evolved in relation to physical spaces: homes, rooms, cabinets, pockets, bags, and vehicles. Searches of the folders and files stored on computers are of course different in many ways. It is unclear to what extent these differences should matter when determining whether the searches and seizures of computer databases are permissible under the Fourth Amendment. Perhaps this question arises most prominently in the controversy over when government officials may properly search and seize "intermingled" documents – documents that are outside the scope of a search warrant, but so intermingled with materials specified in the warrant that on-site separation would be impractical.

A. Differences between Physical and Computer Searches

Professor Orin Kerr has pointed to several ways in which searching computers differs from searching physical spaces.[5] First, government agents obtain information from computers and from physical spaces in different ways. The agent searching a physical space does so by entering a room or opening a drawer and looking around. In the case of computer searches, the agent acquires

[5] Orin Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 538-47 (2005).

information by entering commands into the computer. The computer then passes an electric current over intricate sequences of magnetized points on a hard drive, where the desired information is recorded; then processes the data and sends it – perhaps as text or an image – to an output device, such as a monitor.[6] The manner in which one accesses information from a computer is thus fundamentally different from our traditional understanding of what it means to "search" a place. Describing computer searches in the same terms that we use to describe physical searches is an exercise in analogy.

Second, physical searches involve the examination and occasional seizure of a suspected person's property, while government agents typically acquire computerized information by making an exact duplicate of a target's hard drive, and analyzing the contents of that duplicate on a government computer.[7] Whether copying a suspect's hard drive constitutes a seizure and whether analyzing the contents of the duplicate on a government computer constitutes a search could be matters of reasonable debate.[8] Additionally, some have raised the concern that "law enforcement officers, unencumbered by the type of time pressures attendant to doing a search of a physical premises, might be tempted to rummage through a computer's files well beyond the scope of a warrant."[9]

Third, because computers can store massive quantities of data, the scope of computer searches is potentially much greater. Personal home computers sold at the time of this writing routinely feature one hundred gigabytes of hard drive storage space. This is the equivalent of fifty million typed pages,[10] enough to fill one floor of the average academic library.[11] Physical searches, limited in scope by the sizes of the locations that are searched, will often implicate far fewer documents. The potentially broad scope of a computer search is in tension with the core Fourth Amendment principle that the

---

[6] *Id.* at 538-40.
[7] *Id.* at 540.
[8] *Id.* at 541.
[9] *United States v. Vilar*, 2007 U.S. Dist. LEXIS 26993, 114 (S.D.N.Y. 2007).
[10] One gigabyte of memory space can hold the equivalent of 500,000 typed pages. Nathan Drew Larsen, *Evaluating the Proposed Changes to* Federal Rule 37*: Spoilation, Routine Operation and the Rules Enabling Act*, 4 NW. J. TECH & INTELL. PROP. 212, 216 (2006).
[11] Orin Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 542 (2005).

government agents shall not conduct "general" searches and that warrants shall state with particularity the places they may search and the things that they may seize.[12]

Fourth, physical and computer searches differ in the techniques used for finding evidence. Agents looking for physical evidence work in groups, moving from location to location and conducting their search according to the size of the objects they are trying to find.[13] Computer searches involve the use of programs designed to locate desired information.[14] A government computer analyst may conduct a "logical" search of a computer's data by examining only certain types of files, such as those with a particular extension.[15] Alternatively, the analyst may conduct a "physical" search of the computer's hard drive, examining the file headers that identify for the computer the types of files in storage. This search might pick up partially deleted files and files with altered extensions.[16]

Special problems arise in this area. For example, a person might encrypt the data on his computer, rendering it inaccessible to anyone who could not enter a designated password.[17] It has even been suggested that a computer owner could plant "booby traps" that would cause data to be destroyed if the government computer analyst did not scrupulously follow a preset procedure for accessing the data.[18] These aspects of computer searches make it difficult to chart a course of action for retrieving evidence *ex ante*.[19] Because the target of an investigation could have instituted measures to frustrate a

---

[12] *See Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294, 301 (1967); Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 78 (1994) ("the massive storage capacity of modern computers creates a high risk of overbroad, wide-ranging searches and seizures.").
[13] Kerr, *supra* note 11, at 543.
[14] *Id.* at 534.
[15] *Id.* at 544.
[16] *Id.* at 545.
[17] Orin Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 546-57 (2005).
[18] *See Comprehensive Drug Testing v. United States*, 473 F.3d 915, 946 (9th Cir. 2006) (Thomas, J., dissenting) (citing a government affidavit to this effect).
[19] *See Hill*, 322 F. Supp. 2d at 1090-91 (rejecting defendant's argument that the search warrant was overbroad for failing to articulate a strategy for searching his computer; articulating such a strategy was impracticable because defendant could have easily hidden the contraband under misleading file names).

search for evidence on his computer, there is always the potential that the computer search will be extremely time consuming and invasive.[20]

These differences can make applying search and seizure principles developed in the context of physical searches, at best, an awkward fit for computer searches. This is well-illustrated in the problem of how to treat intermingled documents stored on computer databases.

B. The Problem of Intermingled Documents

This problem arises when government agents serving a valid warrant seize documents not covered in the warrant either because it is not immediately apparent that these documents are outside the scope of the warrant or because these "irrelevant" documents are so commingled with documents covered in the warrant that separating them on-site would be unduly time consuming and intrusive. Tales of these kinds of seizures end up in the federal reporters when the "irrelevant" documents contain evidence of a crime that the search warrant did not contemplate. Once convicted of this new crime on the basis of the inadvertently seized evidence, defendants typically move to suppress, claiming that the initial search was unconstitutional because it exceeded the scope of the warrant.

1. Physically Intermingled Documents

In *United States v. Beusch*, customs officials executed a warrant at a defendant's office.[21] There, they seized two ledgers and a file containing information that fell outside the scope of the warrant, but which prosecutors used as the basis for their convictions.[22] The court rejected defendants' motion to suppress because each of the seized items also contained evidence covered under the warrant[23] and because it would be unduly time consuming and intrusive to require government agents to separate irrelevant from relevant documents contained in a single volume of text.[24] Here, the court observed

[20] Kerr, *supra* note 17, at 547.
[21] 596 F.2d 871, 874 (9th Cir. 1979).
[22] *Id.* at 876.
[23] *Id.* at 877.
[24] *Id.* at 876.

that "[t]he fact that an item seized happens to contain other incriminating information not covered by the terms of the warrant does not compel its suppression, either in whole or in part."[25] The court emphasized in conclusion, however, that its ruling applied to "single files and single ledgers, i.e., single items which, though theoretically separable, in fact constitute one volume or file folder." The court explained that its rationale for allowing seizure in this case may not apply to "sets of ledgers or files."[26]

The Ninth Circuit later took up the question of how to treat "sets" of ledgers and files in *United States v. Tamura*.[27] In *Tamura*, government agents executing a warrant searched defendant's office for specific sales contract, payment, and travel records.[28] Initially unable to locate these documents, the agents seized dozens of boxes and drawers of documents and removed them to another location, where they extracted the relevant materials.[29] The court found this seizure unreasonable. It explained that though agents may inspect all files in a set when searching for documents specified in a warrant, "the wholesale *seizure* for later detailed examination of records not described in a warrant is significantly more intrusive, and has been characterized as 'the kind of investigatory dragnet that the fourth amendment was designed to prevent.'"[30] In dicta, the court suggested that when documents are so intermingled that agents can not feasibly sort them on-site, they may avoid running afoul of the Fourth Amendment by sealing the documents pending a magistrate's approval of a further search.[31]

2. Intermingled Documents on Computers

Every computer search potentially poses an intermingled documents problem. Because computer users may store evidence of criminal conduct on their computer under false file names, inside

---

[25] *Id.* at 877.
[26] *Id.*
[27] 694 F.2d 591 (9th Cir. 1982).
[28] *Id.* at 594.
[29] *Id.* at 595.

[30] *Id.* (emphasis in original), *quoting United States v. Abrams*, 615 F.2d 541, 543 (1st Cir. 1980); *see also United States v. Shilling*, 826 F.2d 1365, 1369-70 (4th Cir. 1987) (Government's desire to keep evidence intact did not condone the seizure of a file cabinet containing numerous documents that the warrant did not cover).
[31] *Id.* at 595-96.

misleading folders, or with different extensions, separating files that fall within the scope of a warrant from irrelevant files often requires time consuming, off-site computer forensic work.[32] To be sure, there are analogous means of frustrating the government's search for physical documents; one might argue that any physical search for documents potentially presents the same issue.[33] Yet perhaps because of the ease with which a person could impede attempts by others to locate evidence on her computer, many courts have allowed law enforcement officers to conduct comprehensive searches of computer storage systems in order to locate relevant documents.[34] On the other hand, courts have also been wary of permitting such broad computer searches, mindful that they would often allow government agents access to a far greater quantity and variety of information about people's private lives as compared to physical searches.[35] Courts have applied a number of doctrines and principles in an effort to balance these concerns.

A few courts have scrutinized the state of mind of the agent who conducted the search, inquiring into whether he uncovered computer evidence of a new crime in the natural course of his search for evidence specified in the warrant or whether he found this evidence because of his efforts to

---

[32] *United States v. Hill*, 322 F. Supp 2d 1081, 1090-91 ("There is no way to know what is in a [computer] file without examining its contents, just as there is no sure way of separating talcum from cocaine except by testing it.").

[33] *United States v. Gray*, 78 F. Supp. 2d 524, 528 (E.D. Va. 1999) (because "few people keep documents of their criminal transactions in a folder marked 'crime records' . . . agents authorized by warrant to search a home or office for documents containing certain specific information are entitled to examine all files located at the site to look for the specified information.").

[34] *See United States v. Vilar*, 2007 U.S. Dist. LEXIS 26993, 115 (S.D.N.Y. 2007) ("Nefarious documents can be given innocuous names, or can be manipulated, hidden or deleted with great ease."); *United States v. Hill*, 322 F. Supp 2d 1081, 1090 (C.D. Cal. 2004) ("[Computer] [i]mages can be hidden in all manner of files, even word processing documents and spreadsheets. Criminals will do all they can to conceal contraband, including the simple expedient of changing the names and extensions of files to disguise their content from the casual observer."); *United States v. Hunter*, 13 F. Supp 2d 574, 583 (D. Vt. 1998) ("Computer records are extremely susceptible to tampering, hiding, or destruction, whether deliberate or inadvertent."); *Gray*, 78 F. Supp. 2d at 529 ("hackers often intentionally mislabel files, or attempt to bury incriminating files within innocuously named directories.").

[35] *See United States v. Walser*, 275 F.3d 981, 986 (10th Cir. 2001) ("Because computers can hold so much information touching on many different areas of a person's life, there is a greater potential for the 'intermingling' of documents and a consequent invasion of privacy when police execute a search for evidence on a computer."); *Hunter*, 13 F. Supp 2d at 583 ("With their unparalleled ability to store and process information, computers are increasingly relied upon by individuals in their work and personal lives. Computer searches present the same problem as document searches – the intermingling of relevant and irrelevant material – but to a heightened degree."); Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 105(1994) ("[the] quantity and variety of information [on a computer] increases the likelihood that highly personal information, irrelevant to the subject of the lawful investigation, will also be searched or seized.").

exceed the authorized scope of the search. In *United States v. Carey*, a police officer searching defendant's computer for evidence of a drug crime came across an image of child pornography.[36] The officer admitted that when he opened other image files, he was looking for child pornography, not for evidence relevant to the warrant.[37] On these facts, the court found that the officer conducted an unconstitutional general search that required suppression of the child pornography evidence.[38] By contrast, in *United States v. Gray*, an FBI agent's inadvertent discovery of child pornography on defendant's computer during the course of his search for evidence of computer hacking was not beyond the scope of the warrant.[39]

For its part, the government has consistently invoked the "plain view" exception to the warrant requirement to argue that it had authorization to obtain computer evidence falling outside the scope of a warrant.[40] This doctrine, which arose in the context of physical searches, provides that the Fourth Amendment does not bar the use of evidence discovered without the authority of a warrant if (1) the officer was lawfully in the place where he discovered the evidence, (2) the incriminating nature of the evidence was "immediately apparent", and (3) the officer has a "lawful right of access to the object itself."[41] As applied to computers, courts have given this doctrine a mixed reception. Despite the fact that viewing a computer image file usually requires entering commands into the computer, some courts have found that the incriminating nature of images of nude children was "immediately apparent" to

---

[36] 172 F.3d 1268, 1271 (10th Cir. 1999).
[37] *Id.* at 1274.
[38] *Id.* at 1276.
[39] 78 F. Supp. 2d 524, 529 (E.D. Va. 1999); *accord United States v. Hollins*, 174 Fed. Appx. 854, 855-56 (5th Cir. 2006).
[40] *See*, *e.g.*, *Carey*, 172 F.3d at 1272; *United States v. Stierhoff*, 2007 US Dist LEXIS 18846, 56 (D.R.I. 2007); *United States v. Anderson*, 2007 U.S. Dist. LEXIS 28329, 17 (D. Ind. 2007).
[41] *Horton v. Cal.*, 496 U.S. 128, 136-137 (1990).

officers who discovered such files.[42] Other courts have found that a computer file is not in plain view when a government agent must enter commands into the computer in order to access the file.[43]

Defendants have argued that there are heightened privacy concerns at stake in a computer search because of the quantity and variety of data computers can store, and therefore, courts should restrict the scope of computer searches.[44] Accordingly, a few courts have issued warrants that restrict the manner in which government agents may search computers.[45] In *United States v. Camlimlim*, for example, the court had issued a warrant requiring the government to use search methods that would avoid exposing documents not included on the warrant.[46] Permitted methods included, surveying file directories, opening files and cursorily reading the first few pages to determine their contents, scanning storage space for intentionally deleted data, and performing key word searches to locate relevant documents.[47] Most courts to have considered the question, however, rejected *ex ante* restrictions on how government agents may search computers.[48] As explained in *United States v. Vilar*, such restrictions would put the court in the position of telling the government how to run its investigation, something it is not qualified to do.[49] The court in *Vilar* also argued that requiring the government to tailor its search by the use of key word searches would "inevitably immunize criminals" because such searches would

---

[42] *See*, *e.g.*, *United States v. Wong*, 334 F.3d 831, 838 (9th Cir. 2003); *Frasier v. State*, 794 N.E.2d 449, 465-66 (Ind. Ct. App. 2003).

[43] *See, e.g.*, *United States v. Lemmons*, 282 F.3d 920, 925 n.5 (7th Cir. 2002) (the police officer's testimony indicated that images of child pornography were not in plain view because he "had to access them by opening a program and looking on the hard drive for pornographic images."); *United States v. Comprehensive Drug Testing*, 473 F.3d 915, 966-67 (9th Cir. 2006) (Thomas, J., dissenting) (computer evidence was not in plain view given that locating this evidence "required analysis and thorough examination off-site."); *see also United States v. Carey*, 172 F.3d 1268, 1271 (10th Cir. 1999) (not deciding whether the plain view doctrine applies to computer searches, but noting that the computer evidence at issue was not in plain view because the officer had to open the files to view their contents).

[44] *See, e.g., United States v. Hill*, 322 F. Supp 2d 1081, 1090 (C.D. Cal. 2004) (defendant argued that government's search of his computer for child pornography should have been restricted to files associated with images, such as those with a ".jpg" suffix, and those with key words such as "sex").

[45] *See, e.g., United States v. Skirving*, 2005 U.S. Dist. LEXIS 38854, 3-4 (D. Or. 2005); *In re Search of 3817 W. West End*, 321 F. Supp. 2d 953, 961 (N.D. Ill. 2004); *United States v. Barbuto*, 2001 U.S. Dist. LEXIS 25968 (D. Ut. 2001).

[46] 2005 U.S. Dist. LEXIS 28002, 47-48 (E.D. Wis. 2005).

[47] *Id.* at 48.

[48] *United States v. Vilar*, 2007 U.S. Dist. LEXIS 26993, 124-25 (S.D.N.Y. 2007) (describing this as the majority view); *Hill*, 459 F.3d at 978 ("[T[here is no case law holding that an officer *must* justify the lack of a search protocol in order to support issuance of the warrant."); *United States v. Brooks*, 427 F.3d 1246, 1251 (10th Cir. 2005) ("[W]e disagree with Brooks that the government was required to describe its specific search methodology.").

[49] *Vilar*, 2007 U.S. Dist. LEXIS 26993 at 124.

leave out many relevant documents, including encoded files and those that employed abbreviations instead of the key words.[50]

Finally, some courts have invoked the *Tamura* court's suggestion, finding that the best way to ensure that the government does not run afoul of the Fourth Amendment in a search that involves intermingled computer documents is for its agents to seal the evidence, pending a magistrate's decision as to the conditions and limits on any further search, and for them to specify to the magistrate in a further warrant what types of files they seek.[51] The Third Circuit went further, modeling its solution on Model Code of Pre-Arraignment Procedure §§220 (1975), which provides for sealing all intermingled documents, pending a hearing at which the defendant may move for the return of some or all of the seized materials.[52]

In sum, courts have articulated many possible ways of balancing the competing concerns at stake when the government conducts a search of intermingled computer documents. Interestingly, although courts repeatedly analogize to principles that guide and limit physical searches in striking this balance, the concerns at issue here are part and parcel of computer technology and the ways that people use computers. One concern is that a defendant will exploit the elaborate filing system that his computer affords in order to hide evidence of his criminal conduct on his computer. This suggests that the government should be free to inspect the entirety of a defendant's computer storage device, without limitation. Moreover, the government has argued, any evidence of criminality that its agents discover along the way should be fair game for further prosecutorial action.

---

[50] *Id.* at 125.
[51] *United States v. Carey*, 172 F.3d 1268, 1275 (10th Cir. 1999); *United States v. Campos*, 221 F.3d 1143, 1148 (10th Cir. 2000); *United States v. Barbuto*, U.S. Dist. LEXIS 25968, 11 (D. Ut. 2001); *United States v. Stierhoff*, 2007 US Dist LEXIS 18846, 56 (D.R.I. 2007).
[52] *United States v. Ninety-Two Thousand Four Hundred Twenty-Two Dollars & Fifty-Seven Cents*, 307 F.3d 137, 154 (3d Cir. 2002).

The other concern stems from the facts that computers have a tremendous capacity to store information and that people tend to document many aspects of their lives on individual computers.[53] These facts suggest that government searches of computers will more often result in "bonus" evidence about previously unknown crimes. Some might argue that permitting the government to acquire evidence of crimes about which it had no reasonable suspicion simply because this evidence happens to reside on a computer storage device designated on a warrant amounts to an arbitrary and dramatic contraction of Fourth Amendment protections.

Unsettled and controversial as this law is, the Ninth Circuit's decision in *United States v. Comprehensive Drug Testing* adds a twist – the problem of intermingled documents containing private information about unrelated third parties – and raises the stakes. In this case, the documents specified in the warrant resided on a large database containing confidential and potentially incriminating information relating to numerous persons about whom the government initially had no suspicions of criminality. The gravity of the decision, which overturned three district courts that had denounced the government's seizure of all of the information in the database, is illustrated by Judge Sidney Thomas' lengthy and vitriolic dissent, in which he wrote, "[t]he majority's holding . . . puts' Americans' most basic privacy interests in jeopardy."[54]

III. United States v. Comprehensive Drug Testing

A. Facts

In connection with the grand jury investigation of the Bay Area Lab Collective ("Balco") and its alleged distribution of illegal steroids to major league baseball players, the United States government executed warrants at two commercial drug testing labs, seeking the drug testing records of ten players.[55]

---

[53] Orin Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 569 (2005) ("Today [computers] are postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more.").
[54] *United States v. Comprehensive Drug Testing, Inc.*, 473 F.3d 915, 963 (9th Cir. 2006).
[55] *Id.* at 919-22.

These labs had analyzed the confidential drug testing results for all professional baseball players pursuant to a collective bargaining agreement between Major League Baseball and the Major League Baseball Players Union ("Players Union"), the purpose of which was to assess whether an individualized steroid testing program was necessary.[56]

As the warrant at issue authorized, the government made duplicates of the labs' computer databases, and, back in its offices, searched these databases for evidence specified in the warrant.[57] The information in these databases included not only data on the ten professional baseball players specified in the warrant, but also drug testing records for every professional baseball player, and medical records for persons in thirteen other sports organizations, three business entities, and three sports competitions.[58] On the basis of the information in these databases, the government later obtained additional search warrants to seize materials relating to over one hundred professional baseball players who had been listed as testing positive for steroids.[59]

In response to these actions, the Players Union filed motions in two federal courts, pursuant to Federal Rule of Criminal Procedure 41(g), seeking the return of the seized property.[60] These courts granted the Players Union's motions, ordering the government to return all materials not pertaining to the ten players named in the initial warrant.[61] A third federal court, at the Players Union's behest, quashed the government's subpoena for records pertaining to the over one hundred players who tested positive for steroid use.[62] On consolidated appeal, Judge Diarmuid O'Scannlain, joined by Judge Richard Tallman, overruled all three lower courts.

---

[56] *Id.* at 944-45.
[57] *Id.* at 921-23.
[58] *Id.* at 944.
[59] *Id.* at 923-24.
[60] *Id.* at 923; Federal Rule of Criminal Procedure 41(g) provides for "a person aggrieved by an unlawful search and seizure of property" to move for the property's return.
[61] *Id.* at 924.
[62] *Id.* at 925.

B. The Majority Opinion

As an initial matter, after weighing the factors put forth in *Ramsden v. United States*,[63] the court found that the lower courts had equitable jurisdiction to hear and rule on the 41(g) motions.[64] The court reached this conclusion despite its determination in respect to one of the *Ramsden* factors that the government had not displayed a callous disregard for the plaintiff's constitutional rights.[65] The court's discussion on this subsidiary point was important because it drove its decision on the merits.[66]

The court listed a series of reasons for its finding that the government's seizure of intermingled documents did not show callous disregard on the part of the government.[67] It pointed to the agents' compliance with the warrant's "protective procedures," which called for a government computer technician to determine whether the computer materials were so intermingled as to require off-site analysis.[68] It noted that, unlike in *Tamura*, the seized documents were pertinent to the Balco investigation and that the agents did not seize the materials in order to coerce plaintiff's cooperation.[69] It also determined that the agents removed the documents for off-site review, not because they were insensitive to the privacy rights at stake, but because this would be less disruptive to the drug testing lab.[70] Finally, the court rejected the notion that the agents should have relied on the lab's guidance in pointing them to the pertinent computer files, reasoning that the lab, "[l]ike most searched parties," had an incentive to withhold documents from the government.[71]

On the merits, the court dispensed with the 41(g) motions in short order, ruling that the government may keep all of the evidence so long as it needs it and its conduct in acquiring the evidence

---

[63] 2 F.3d 322, 325 (9th Cir. 1993).
[64] *Comprehensive Drug Testing*, 473 F.3d at 936.
[65] *Id.*
[66] *Id.* at 959 (Thomas, J., dissenting) ("Because the equitable jurisdictional analysis in large part drives the analysis of the merits of the *Rule 41(g)* decisions, it is important to detail my differences with the majority on this issue.").
[67] *Id.* at 933-34, 936.
[68] *Id.* at 933-34.
[69] *Id.* at 934.
[70] *Id.*
[71] *Id.* at 935.

was not "sufficiently reprehensible."[72] But as a separate matter, drawing on *Tamura*,[73] the court went on to rule that the Fourth Amendment required that the seizure and off-site review of intermingled computer documents be supervised by a neutral magistrate judge.[74] Importantly, the court did not require that a magistrate step in to review the evidence as soon as the government learns that the relevant database contains intermingled documents. Rather, the court designed a trigger; magistrate review would occur only upon a "proper post-seizure motion by the aggrieved parties."[75]

The magistrate's role would then be to "filter the evidence off-site," determining which documents fall within the scope of the warrant. In going about this filtering process, the court directed that the magistrate "apply our precedent, including *Beusch*, which permits the seizure of single ledgers or files with intermingled data." The court went on to suggest that most computer files can be "pared down considerably," but "certain files – spreadsheets of only a few pages, for example – may be retained in whole."[76] The court elaborated that

> [i]n this analysis, the magistrate may consider relevant, among other factors: 1) whether evidence mentioned in the search warrant can be separated from unrelated evidence by copying or moving files, but without creating new documents, 2) whether the file, if printed, would fill more than a typical paper ledger (of the sort in *Beusch*), 3) whether excision of the unrelated portions of the document would distort the character of the original document. This list is neither exhaustive nor mandatory, but offers relevant considerations for a magistrate to determine what evidence the government can reasonably retain after a lawful seizure of intermingled digital data.[77]

Once the magistrate has set aside evidence covered under the warrant, the government would be able to retain and use this evidence. It would have to return the rest of the evidence to the aggrieved party. The government, however, would be free to seek additional warrants to pursue an expanded

---

[72] *Id.* at 937-38.
[73] *United States v. Tamura*, 694 F.2d 591, 595-96 (9th Cir. 1982).
[74] *Comprehensive Drug Testing*, 473 F.3d at 938.
[75] *Id.* at 939.
[76] *Id.* at 940.
[77] *Id.* at 940 n.45.

investigation on the basis of evidence of criminality that it uncovered during its initial review of the seized evidence.[78]

C. The Dissent

Judge Thomas, dissenting, argued that the government had shown a callous disregard for the constitutional rights of the Players Union because the government had sought numerous warrants as an end run around the Players Union's motion to quash a subpoena for the wholesale seizure of the lab data,[79] it made misleading statements in its applications for these warrants,[80] and these warrants were a mere pretext for inappropriately obtaining medical information about professional baseball players not under any particularized suspicion of criminal conduct.[81] The dissent's "most profound disagreement" with the majority, however, was on the question of whether the government was entitled to seize all of the medical information because it was intermingled with information specified on the warrant.[82] He argued that the majority's conclusion squarely conflicted with *Tamura*, which condemned "the wholesale *seizure* for later detailed examination of records not described in a warrant,"[83] because in this case the agents knew they were seizing large amounts of data not specified in the warrant, including information on approximately 1,200 players.[84] The dissent dismissed the majority's attempt to distinguish *Tamura* on the ground that the seizure of a copy of the computer database was not disruptive to the testing lab's business, noting that in this case the countervailing interest was one of privacy, not of disruption of business operations, such that seizing a copy imperiled the interest just the same.[85]

---

[78] *Id.* at 940.
[79] *Id.* at 959.
[80] *Id.* at 960.
[81] *Id.* at 961.
[82] *Id.* at 962.
[83] *United States v. Tamura*, 694 F.2d 591, 595 (9th Cir. 1982).
[84] *Comprehensive Drug Testing*, 473 F.3d at 963.
[85] *Id.*at 963 n.9.

Coming to the heart of his grievance, Judge Thomas argued that the majority's approach, which incorrectly applied *Beusch* in the computer context, "would permit the government to seize *all* the documents on a given computer if only one document therein was responsive to the warrant."[86] This result "puts Americans' most basic privacy interests in jeopardy" because it "would entitle the government to seize the medical records of anyone who had the misfortune of visiting a hospital or belonging to a health care provider that kept patient records in any sort of master file which also contained the data of a person whose information was subject to a search warrant."[87] Calling this state of affairs "staggering," he charged that the majority's holding meant that "no laboratory or hospital or health care facility could guarantee confidentiality of records."[88]

The better option, which Judge Thomas argued is true to *Tamura*, would be to require that a magistrate "examine the co-mingled data that the government proposes to seize to make sure that private information that the government is not authorized to see remains private."[89] He indicated that the magistrate would not necessarily conduct a direct filtering of the relevant evidence; instead, when agents anticipate that they will encounter intermingled computer evidence or when they encounter such evidence unexpectedly, they should seek a magistrate's "guidance on how to proceed."[90] The majority criticized this approach, contending that it would force agents unexpectedly confronted with intermingled evidence to "give up the search and leave." They would then have seek a further search warrant to remove the intermingled evidence, repeating this process until it obtained all the relevant materials, at which point the intermingled evidence "might well no longer be intact."[91] Elsewhere in his

[86] *Id.*
[87] *Id.* at 963-64.
[88] *Id.* at 964.
[89] *Id.* at 965.
[90] *Id.* at 964-65.
[91] *Id.* at 939.

opinion, however, the dissent appeared to address this concern by his suggestion that government agents could also transfer all of the data to the magistrate for "segregation and management."[92]

Judge Thomas took issue with the majority's procedure that required magistrate review upon the objection of a party. First, he contended that the protections afforded by the review of a "neutral and detached magistrate" are lost when this review occurs after the government has already searched and seized the materials.[93] Second, he pointed out that that if no "proper post-seizure motion by the aggrieved parties" is made, there will never be magistrate review, and the government would be free to continue searching all of the documents, irrespective of whether they had seized them with particularized suspicion of criminal activity.[94] This was an especially troubling prospect in the case of documents pertaining to unrelated third parties, because these persons may not know that the government had taken records pertaining to them, and they therefore would not know to object.[95] Moreover, the dissent complained that the majority's approach required these third parties to undertake the burdensome steps of hiring an attorney and making a "proper post-seizure motion."[96]

Finally, the dissent found that the majority's guidelines for the magistrate's filtering of relevant documents, including that it do so without creating new documents or distorting the character of original documents, were not sufficiently protective of the privacy rights of innocent third parties and ignored the realities of computer storage systems.[97] Judge Thomas wrote, "[u]nder the majority's approach, the government would be entitled to retain all electronic information if 'co-mingled.' Given that 'co-mingling' is an inherent aspect of electronic databases, this restriction renders the *Fourth*

---

[92] *Id.* at 976 n.19.
[93] *Id.* at 974 ("For a magistrate's role to be effective, it must come before the privacy interests have been compromised. Under the majority's holding, the government is newly empowered to search the data *before* the magistrate authorizes the search.").
[94] *Id.*
[95] In fact, this was precisely what occurred in this case; records of players in the National Hockey League were among those that the government seized from a drug testing lab, yet until this opinion, no one in the National Hockey League knew that the government had seized these records. *Id.*
[96] *Id.* at 975.
[97] *Id.*

Amendment a nullity in the electronic context."[98] The better approach, he argued, would be for the government to take advantage of software programs allowing the "examination and correlation of information" in order to separate irrelevant materials. For example, the government could have used key word searches to retrieve information responsive to the search warrants.[99] The majority countered this suggestion with its observation that "key word" searches could have left much relevant evidence undiscovered, such that searching the entire computer database was necessary "to seek out all the evidence covered by the search warrant."[100] But the dissent also suggested another, "better" alternative: the government could have turned the database over to the magistrate for "segregation and management."[101]

D. Analysis

In sum, the majority and the dissent agree that there should be magistrate review when the government, while executing a search warrant, comes across intermingled computer documents. Their key differences are in the timing and nature of this review. In the interest of ensuring that the government is able to fully execute the warrant and locate all relevant evidence, the majority would allow the government to seize, then search, an entire database. Then, upon the proper motion of an aggrieved party, a magistrate would review the database, filtering out the relevant evidence, and returning to the movant the remainder of the data. The government could yet use the information it had obtained up to that point in order to expand its criminal investigation to new crimes and to establish probable cause for further search warrants.

The dissent contended that this approach afforded inadequate Fourth Amendment protections to the persons whose data the government seized, especially those persons as to whom the government lacked any particularized suspicion of criminality. This is because the majority's approach permits the

---

[98] *Id.* 976.
[99] *Id.* at 975.
[100] *Id.*
[101] *Id.* at 976 n.19.

government potentially indefinite access to large quantities of private information, despite the government's lack of any particularized suspicion of criminality, just because this information has been stored on a computer database with other information responsive to a warrant.

By contrast, the dissent contended that when government agents come across intermingled computer evidence, they should discontinue their search and permit a magistrate to first review the database. The magistrate either might instruct the government as to how it should search the database for the relevant materials, so as to minimize the possibility that the government would improperly view information not mentioned in the warrant, or might itself segregate or redact the irrelevant information. The majority dismissed the first of these suggestions on the grounds that targeted, non-comprehensive searches of a database are always potentially incomplete. The second of these suggestions, however, is not dismissed so easily.

Allowing the magistrate to review and segregate the database prior to the government's seizure of the intermingled documents would address the dissent's objection that the government should not be free to access large quantities and varieties of private information on a computer before a warrant gives it authority to do so. Some might object that the magistrate, under this approach, would improperly assume the role of prosecutorial investigator; deciding which documents constitute evidence of criminality as specified in the warrant might at times be a tricky business.[102] Yet the majority itself seems comfortable with this prospect, given that it would require precisely this type of magistrate review upon the objection of an aggrieved party. Put another way, it is unclear why the majority would not require that a magistrate review the entirety of a database containing intermingled computer documents as a default measure, prior to the government's off-site search.

---

[102] *See United States v. Vilar*, 2007 U.S. Dist. LEXIS 26993, 124 (S.D.N.Y. 2007) (counseling that courts should avoid getting into "the business of telling investigators how to conduct a lawful investigation, something the courts are ill-equipped to do.); *cf. United States v. Brooks*, 427 F.3d 1246, 1252 (10th Cir. 2005) (discussing the problems with *ex ante* search protocols for searching computers, noting, "[g]iven the numerous ways information is stored on a computer, openly and surreptiously, a search can be as much an art as a science.").

Some possible reasons come to mind. As an administrative matter, it may be unduly burdensome for magistrates to undertake the onerous task of sifting relevant evidence from gigantic databases whenever the government comes across a database with intermingled documents. As a practical matter, a magistrate's review might be required every time the government searches a computer, since, as the dissent recognized, "'co-mingling' is an inherent aspect of electronic databases."[103] This is not an entirely satisfactory objection. The privacy rights at issue would often seem to take precedence over even these important administrative considerations. Moreover, administrative alternatives are available; the magistrate, for example, could delegate his filtering duties to a special master.[104]

Additionally, one might object that because a magistrate is not likely to know the facts of an investigation as well as a government investigator, the magistrate may at times fail to recognize that some documents are relevant to an investigation. Thus, the magistrate might wrongfully prevent the government from having access to some documents. The majority's approach, perhaps, might offer the advantage of allowing government agents to take a "first cut" at the material on the database and to familiarize themselves firsthand with the sorts of documents it contains. This might help the government to petition the magistrate as to the relevance of materials later withheld. Again, this is not a very satisfactory complaint. When the reviewing magistrate is the same person who issued the initial search warrant, she would not be making relevancy determinations starting with a blank slate. Additionally, the government would presumably be available during the filtering process to assist the magistrate in determining what types of documents are relevant to its investigation. Therefore, this objection is not persuasive, especially in light of the privacy concerns at stake.

---

[103] *Comprehensive Drug Testing*, 473 F.3d at 976.

[104] *Cf. United States v. Abbell*, 914 F. Supp. 519 (S.D. Fla. 1995) (ordering a special master to review materials seized during a search of a law office and to segregate documents protected by the attorney-client privilege)

IV. Constitutional, Statutory and Common Law Protections Against Disclosure Accorded to Personal Information Stored in a Commercial Computer Database

An important aspect of *Comprehensive Drug Testing* was the fact that the evidence specified on the search warrant was intermingled with personal data relating to third parties, who initially were not targets of the government's investigation. It is not clear to what extent this fact weighed in the majority's opinion and in its holding that there be magistrate review of a database containing intermingled evidence. For the dissent, at least, the issue of third party exposure to government scrutiny was crucial. Judge Thomas emphasized that this ruling would have far reaching effects on the health care industry in that it would vastly increase the government's ability to take prosecutorial action against individuals in the absence of particularized suspicion of criminal conduct, effectively undermining the confidentiality of patient information stored on computer databases.[105] In fact, if one takes the dissent's concerns seriously, it is not at all clear why one should single out medical databases. The court's ruling did not hinge on the fact that it was a medical database at issue. Rather, its approach to the treatment of intermingled computer documents would seem applicable to any commercial database on which the information of more than one person is stored.

Because of this decision's sweeping consequences for the privacy rights of persons with personal information stored on the computer databases of businesses and other entities, it is worthwhile to inquire into what those rights are. It turns out that they are very limited.

A. Constitutional Protections

Several pre-Information Age Supreme Court decisions hold that persons do not have a reasonable expectation of privacy in specific types of information that they voluntarily reveal to third parties,[106] such that this information is not entitled to Fourth Amendment protection.[107] The Court has

---

[105] *Comprehensive Drug Testing*, 473 F.3d at 963-64.

[106] *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

found that there is no Fourth Amendment protection for information that an individual reveals to his accountant[108] or to his bank,[109] even when the individual believed that the information would remain confidential.[110] Similarly, the Court has found that persons do not have a reasonable expectation of privacy in the phone numbers that they dial because they know that the telephone company receives this information.[111] These decisions have been invoked more recently for the proposition that persons generally do not enjoy Fourth Amendment protections in any information they voluntarily disclose to a business or organization. Thus, most medical, educational, insurance, and financial records held by businesses may be without constitutional protection, such that in the absence of some statutory bar or common law protection, they may be freely disclosed to the government.[112] Were a court to accept this reasoning, a defendant charged with a crime on the basis of evidence that the government acquired by virtue of the fact that it was intermingled on a database with other information responsive to a warrant, would often be without a basis to suppress this evidence.

Whether this reasoning, derived in the 1970s, is valid as applied to computer databases and electronic transactions is a matter of debate, however, "given the revealing nature of the huge amounts of transactional data generated by electronic systems today."[113] Additionally, a different line of cases, preserving constitutional privacy rights in personal property that an individual leaves on another's premises – so long as that property is secured against others' access and the owner's right of access is limited – suggests that certain types of personal information stored on another's computer database

---

[107] Ari Schwartz et. al., *Storing Our Lives Online: Expanded Email Storage Raises Complex Policy Issues*, 1 ISJLP 597, 602 (2005); *Smith v. Maryland*, 442 U.S. 735, 740 (1979) ("[T]his Court uniformly has held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action.").
[108] *Couch v. United States*, 409 U.S. 322 (1973).
[109] *United States v. Miller*, 425 U.S. 435, 443 (1976) ("The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.").
[110] *Id.* ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.").
[111] *Smith*, 442 U.S. at 742.
[112] Schwartz, *supra* note 107, at 602.
[113] *Id.*

may yet enjoy constitutional protections.[114] Moreover, one's privacy protections in information disclosed to an outside entity are likely to vary depending on the type of information at stake.[115]

On the other hand, defendants charged with crimes on the basis of evidence that the government acquired as a "bonus" when executing a warrant for an unrelated investigation may have to overcome a further obstacle in order to invoke the exclusionary rule. In a line of cases, the Supreme Court has held that defendants may not obtain a suppression remedy merely because the government violated a third person's Fourth Amendment rights.[116] Apart from the question of whether a defendant had a reasonable expectation of privacy in personal information stored in a commercial database, courts may question whether it is the defendant's or the database administrator's Fourth Amendment rights that have been violated when the government engages in an allegedly unconstitutional search of such a database. Where it is the database administrator's rights at issue, a court would likely deny the defendant a suppression remedy.

B. Statutory Protections

Apart from whether personal information stored in a computer database enjoys constitutional protection against disclosure, there are some statutory protections against disclosure. Where such a statute applies to the digital information at issue, a court may be more willing to restrict the government's access. Usually, however, the government's violation of a regulatory statute does not give

---

[114] Patricia L. Bellia, *Surveillance Law through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1405 (2004); *see, e.g.*, *United States v. Johns*, 851 F.2d 1131 (1988) (reasonable expectation of privacy in a rented storage unit).

[115] *See* Sam Kamin, *The Private Is Public: The Relevance of Private Actors in Defining the Fourth Amendment*, 46 B.C. L. REV. 83, 133 (2004) (noting a split in the courts prior to the passage of federal privacy laws about whether persons had a reasonable expectation of privacy in their medical information).

[116] *United States v. Payner*, 447 U.S. 727, 735 (1980) ("Fourth Amendment decisions have established beyond any doubt that the interest in deterring illegal searches does not justify the exclusion of tainted evidence at the instance of a party who was not the victim of the challenged practices."); *Rakas v. Illinois*, 439 U.S. 128, 134 (1978) ("A person who is aggrieved by an illegal search and seizure only through the introduction of damaging evidence secured by a search of a third person's premises or property has not had any of his Fourth Amendment rights infringed."); *Alderman v. United States*, 394 U.S. 165, 174 (1969) ("Fourth Amendment rights are personal rights which, like some other constitutional rights, may not be vicariously asserted.").

the defendant a suppression remedy.[117] Thus, a defendant charged with a crime on the basis of evidence seized in violation of a protective statute would usually be no better off.

For example, subject to certain exceptions, the Family Education Rights and Privacy Act prohibits educational institutions from disclosing a student's educational records without parental consent.[118] In *United States v. Bunnell*, the court found that there was no suppression remedy for a violation of this statute.[119] The plain language of the statute supports this interpretation, for there is no mention of a suppression remedy, and the statute in fact mentions a different remedial scheme: the withdrawal of federal funds from institutions that violate the statute.[120] Another example is the Fair Credit Reporting Act, which limits what consumer reporting agencies may disclose to the government about any consumer.[121] In *United States v. Edgar*, the First Circuit ruled that there is no suppression remedy for the violation of this statute, noting that such a remedy is not mentioned in the act.[122] Additionally, the Stored Communications Act,[123] passed as part of the Electronic Communications Protection Act of 1986,[124] requires that the government obtain stored electronic communications that are less than 180 days old only by means of a warrant.[125] It does not appear, however, that a suppression remedy attaches for violations of this statute either.[126]

---

[117] *See United States v. Lombera-Camborlinga*, 206 F.3d 882, 886 (9th Cir. 2000) ("an exclusionary rule is typically available only for constitutional violations, not for statutory or treaty violations.") (en banc); *United States v. Cooper*, 2005 U.S. Dist. LEXIS 39116, 10 (N.D. Cal. 2005) ("judicially implied exclusionary remedies for statutory violations are disfavored, particularly when Congress has specified other remedies.").
[118] 20 U.S.C.S. § 1232g(b) (2007).
[119] 2002 U.S. Dist. LEXIS 9090, 6 (2002).
[120] 20 U.S.C.S. § 1232g(b)(1) (2007); *Cf. Gonzaga Univ. v. Doe*, 536 U.S. 273, 279 (2002) (Congress drafted FERPA as spending legislation such that it does not confer an enforceable private right action under § 1983).
[121] 15 U.S.C.S. § 1681f (2007).
[122] 82 F.3d 499, 510-11 (1996); 15 U.S.C.S. § 1681n (2007).
[123] 18 U.S.C.S. § 2703 (2007).
[124] 18 U.S.C.S. § 2510 et seq. (2007).
[125] 18 U.S.C.S. § 2703(a) (2007).
[126] *Bansal v. Russ*, 2007 U.S. Dist. LEXIS 25540, 27 n.6 (E.D. Pa. 2007) (noting in dicta that "that the Stored Communications Act does not provide for exclusion of evidence as a remedy.").

On the other hand, certain mental health and substance abuse records are protected against disclosure under federal law,[127] and there is some reason to believe that a court would permit a suppression remedy when the government violates these laws.[128] Additionally, it has been observed that State Constitutions and statutes may further restrict the government's authority to search computer databases.[129]

C. Common Law Protections

It is also possible that the operation of some common law protection against disclosure, especially the attorney-client privilege, would make courts hesitant to grant to the government broad authority to conduct searches of databases containing intermingled documents. Thus, in a line of cases involving search warrants executed in law offices, courts have adopted special measures, similar to those suggested in *Tamura*, to protect against disclosure of privileged materials.[130] In some cases, courts may also be willing to grant a suppression remedy for evidence seized in violation of such protections.[131]

V. Conclusion

Despite its provision for magistrate review, *Comprehensive Drug Testing* leaves a huge gap in the Fourth Amendment protections of private information stored on commercial electronic databases. Until an aggrieved party files a proper post-seizure motion, assuming this ever happens, government

---

[127] 42 U.S.C. § 290dd-2(f) (2007).

[128] *United States v. Shinderman*, 2006 U.S. Dist. LEXIS 33323, 3 (D.Me. 2006) (noting in dicta that "both the statute and the regulations contain broad language that would support suppression for at least some violations.").

[129] Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 101-02 (1994).

[130] *In re Impounded Case* (*Law Firm*), 840 F2d 196, 202 (3d Cir. 1988) ("The attorney-client privilege is sufficiently protected by the procedure established by the magistrate requiring that the government obtain leave of the court before examining any seized items.").

[131] *See United States v. Leon*, 468 U.S. 897, 979 n.38 (noting that "[t]he exclusion of probative evidence in order to serve some other policy is by no means unique to the Fourth Amendment," and mentioning the attorney-client, marital, priest-patient, and doctor-patient privileges.); *United States v. Haynes*, 216 F.3d 789, 797 (9th Cir. 2000) (finding that suppression of evidence seized in violation of defendants' attorney-client privilege was an appropriate remedy); *National City Trading Corp. v United States*, 635 F2d 1020, 1026 (2d Cir. 1980) ("To the extent that the files obtained here were privileged, the remedy is suppression and return of the documents in question."); *Webb v. Walsh*, 2005 U.S. Dist. LEXIS 32319, 26 (E.D.N.Y. 2005) (noting that even if the doctor-patient privilege created a basis for suppression, habeas petitioner's claim was properly denied because of the operation of the independent source doctrine.).

agents are free to review entire commercial electronic databases and engage in follow-up prosecutorial actions without ever having established particularized suspicions of criminality in respect to much of this information. On top of the court's expansion of the permissible scope of a government's search of a commercial electronic database, independent constitutional, statutory, and common law principles provide limited protection for individuals whose private information is seized. Defendants prosecuted on the basis of incriminating information acquired during the course of such seizures will find themselves with few suppression remedies, even if they are able to show that the government's conduct violated a statute.

One way to avoid these problems would be to adopt the dissent's proposal for default magistrate review either when the government anticipated encountering intermingled computer evidence or when it came across such evidence unexpectedly. Alternatively, it may be sensible to operate under the presumption that computer searches will entail encounters with intermingled evidence. In any case, the magistrate should review and segregate the evidence directly, rather than continually offering guidance to the government's agents. Though this approach has its drawbacks, they do not seem insurmountable, nor are they as disconcerting as the results that flow from the Ninth Circuit panel's decision.

One may fairly assume that computers and computer databases will only become more integral tools for organizing and recording our lives. Surely few would argue that a necessary aspect of this dynamic should be a lessening of our protections against the government's authority to search and seize our personal information. The root harm of *Comprehensive Drug Testing* is that it arbitrarily appends to the societal benefits that arise from the use of commercial electronic databases a proportional relinquishment of Fourth Amendment protections. Our fundamental constitutional principles must be more flexible, and sensible, than this.