

# COMPLIANCE WEEK

THE LEADING INFORMATION SERVICE ON CORPORATE GOVERNANCE, RISK AND COMPLIANCE

## **e-Discovery Challenges in Criminal Probes**

By Jaclyn Jaeger — December 23, 2008

The rules of legal discovery in the Internet and e-mail era are rapidly developing for civil litigation. But in the realm of criminal investigations—where the stakes can be far higher—the law still leaves corporations flailing without any way to protect electronic data, even if it belongs to innocent third parties.

The recent Ninth Circuit Court of Appeals opinion *U.S. v. Comprehensive Drug-Testing* (commonly known as the infamous BALCO case, exploring steroid use among professional baseball players) should serve as a wake-up call to Corporate America, experts tell Compliance Week.

In the BALCO probe, government agents executed a search warrant after developing probable cause that the Bay Area Lab Cooperative sold steroids to baseball players. Based on the seized data, government officials also were able to obtain confidential medical records of other players who tested positive for steroids. Agents used that information, in turn, to get more search warrants.

The defendants promptly said the government should not have been able to obtain new search warrants based on electronic data it found but wasn't specifically looking for. The appeals court disagreed, and found that entire collections of computer data can be seized where files within the scope of a search warrant are intermingled with irrelevant data.

“What the BALCO decision tells us is that personal evidence that may have not been identified previously by the government can now be obtained without any prior knowledge ... just because the information happens to share space on a computer with information that was specified under a warrant,” says Justin Murphy, a securities lawyer at the law firm Crowell & Moring who specializes in e-discovery matters.

For corporations, always eager to keep as much control of their electronic data as they can, the BALCO ruling “really raises concerns about the current state of Fourth Amendment privacy protections, and almost takes those concerns to a new level,” says Murphy.

Critics of the BALCO ruling don't stop there. The decision also granted permission for government agents to browse the contents of computer files to determine if they are within the scope of the warrant, without having to limit such a search to keywords or certain types of files.

In a dissent to the ruling, Judge Sidney Thomas voiced fears about Fourth Amendment rights and advocated some sort of magistrate review of intermingled computer files before letting government agents inspect them. And indeed, two other federal court decisions—*U.S. v. Carey* and *U.S. v. Tamura*—have made rulings similar to Thomas’s position.

“The point being that such wholesale removal should be monitored by a neutral and detached judge,” Murphy says. Still, other courts have found that how a search warrant is executed is left to the discretion of the agents, he adds.

Complicating matters in criminal cases is that government officials often assume intent, which can affect a company’s perceived level of culpability and cooperation, Murphy warns. “Government investigators by nature are skeptical and sometimes encounter efforts that companies, or individuals, have made to destroy evidence,” he says.

### **Data Protection**

To protect data that might be swept up in a criminal probe, companies should employ many of the same policies they use to protect data in civil litigation. Most important: have written policies in place that employees can follow, and compliance executives or general counsels can show to prosecutors should they ever pay a visit to the office.

Mary Ann Benson, director of consulting services at Epiq Systems, says companies must always drill home the point that “personal e-mail is not ‘personal’ e-mail” when sent across corporate networks or any company-owned device. “Employees need to really understand that these are corporate assets, and that any data conveyed through them is really owned by the company,” she says.

Other wise policies include document retention plans, legal-hold checklists, and litigation readiness plans. “Many companies believe these types of readiness plans are nice-to-haves, rather than must-haves,” Murphy says.

The cost of *not* having them can be substantial. Section 1519 of Sarbanes-Oxley, for example, establishes fines or imprisonment of up to 20 years if an individual knowingly destroys, alters, or falsifies any record or data to impede the investigation of any investigation. What’s more, the employer of that would-be offender almost certainly would be in violation of Section 404 of Sarbanes-Oxley, which mandates that companies have strong internal controls to prevent fraud from happening in the first place.

Equally important is to ensure that the policies are monitored and enforced. “It’s one thing to bring in a law firm to do a litigation-hold plan, and it looks terrific and tells you everything you need,” Murphy says. “But if you’re not going to enforce and monitor compliance with them, it’s not going to do you a lot of good.”

Benson agrees. “There’s a saying that it’s better to have no document retention policy than to have one that’s not enforced, because if you are found later to have violated your

own policy—whether on purpose or accidentally—you're perceived to be in far greater trouble than if you just didn't have a policy to begin with.”

To that end, companies should name someone at the senior level who can be responsible for enforcing compliance and implement training, Murphy says. “The point is that when litigation arises and you need to implement procedures, you've got a chain of command,” he says.

A senior-level leader also could help improve cooperation between the legal and IT departments, which can be a tricky gap to bridge. “Lawyers often don't understand IT, and IT doesn't understand the legal rules we're operating under,” says Murphy.

### **Third-Party Intervention**

Still, there are instances when having third-party expertise, especially in criminal matters, is essential. For example, Benson says, many companies when faced with a criminal investigation take the initiative to collect documents that they think are relevant. While nothing is wrong with doing this per se, problems can arise when a company has information that it may not want to be confiscated, she says.

Murphy adds that third-party expertise can also help persuade the government that the most pertinent and relevant is being provided, without the need for government agents to show up and turn the business upside-down. “It's very advantageous to have a third-party forensic specialist who can assist with preservation and collection of potentially relevant material, and somebody who can be a testifying witness if needed,” he says.

Where human resources are limited, e-discovery software can aid companies in parsing out relevant documents. If an employee is suspected of fraud, for example, the odds of that person using the word “fraud” in his daily e-mail are pretty small, Benson says. Software search tools can help to deduce what the content and the meaning of different communications are.

E-discovery software can also eliminate duplicated e-mails, or even identify documents that are nearly duplicative. Such a tool allows you to see the final version of a contract, for example, rather than 15 previous drafts, says Benson. She adds that typically, only 15 percent of data collected by companies is relevant.

Companies can reduce duplicative e-mails in other ways. For example, when replying to an e-mail, respond to the sender, rather than hitting “reply to all,” says Benson. In addition, she encourages companies to send links in e-mails, rather than whole documents. “From a compliance perspective, that's just that much less data that they need to worry about, and that many fewer copies of something that they need to maintain control over.”

## BALCO RULING

**The following excerpt is from *United States vs. Comprehensive Drug Testing*.**

We see no evidence of bad faith or pretext here.

Nor does the seizure of intermingled documents demonstrate “a callous disregard for the constitutional rights of the movant.” Ramsden, 2 F.3d at 325 (stating the first factor weighing in favor of equitable jurisdiction over a motion for return of property). In this analysis, we focus on the Fourth Amendment and note that “[a]s always under the Fourth Amendment, the standard is reasonableness.” *United States v. Hill*, 322 F. Supp. 2d 1081, 1088 (C.D. Cal. 2004) (Kozinski, Circuit J., sitting by designation). Reasonableness can be especially difficult to define in the computer context, given the well-known “difficulties of examining and separating electronic media at the scene.” *Hill*, 322 F. Supp. 2d at 1090. Fortunately, our prior precedent reveals that agents can avoid the opposing errors of leaving behind essential information and sweeping up excessive evidence.

In *United States v. Beusch*, 596 F.2d 871 (9th Cir. 1979), this court addressed a motion to suppress seized evidence consisting of ledgers containing items covered by the search warrant intermingled with items not covered by the search warrant. *Id.* at 876-77. The *Beusch* court concluded that no Fourth Amendment violation occurred when agents seized “single files and single ledgers, i.e., single items which, though theoretically separable, in fact constitute one volume or file folder.” *Id.* at 877.

The *Beusch* court expressly limited its reach, however: “[T]he reasons we have given for allowing [such] seizure may not apply to sets of ledgers or files, but because that is not the case here, we find it unnecessary to discuss it further.” *Id.* Three years later, the court addressed the seizure of sets of files. *See Tamura*, 694 F.2d 591. In *Tamura*, the court reviewed the conduct of officers executing a search warrant, which authorized seizure of three specific categories of records from a Los Angeles office. *Id.* at 594. In that case, agents seized—without any limiting effort—files unrelated to the items mentioned in the search warrant. *Id.* at 595. The *Tamura* court condemned such “wholesale seizure for later detailed examination of records not described in a warrant.” *Id.*

Unfortunately, the *Tamura* court did not answer a more difficult question: “Because seizable materials are seldom found neatly separated from their non-seizable counterparts, how much separating must police do at the scene to avoid taking items that are neither contraband nor evidence of criminal activity?” *Hill*, 322 F. Supp. 2d at 1088. As the *Hill* court noted, the answer turns upon “reasonableness,” *id.*, a standard that offers little guidance to government agents. Understandably, the *Tamura* court sought to give more concrete advice to help agents remain within the bounds of the Fourth Amendment.

The court suggested:

In the comparatively rare instances where documents are so intermingled that they cannot feasibly be sorted on site, we suggest that the Government and law enforcement officials generally can avoid violating fourth amendment rights by sealing and holding 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-Arrestment Procedure.

### Source

United States vs. Comprehensive Drug Testing (Balco) (Dec. 27, 2006).

---

Compliance Week provides general information only and does not constitute legal or financial guidance or advice.