

---

## Government "Taint Teams" May Open a Pandora's Box: Protecting Your Electronic Records in the Event of an Investigation

2004-05-11

Law enforcement agents routinely seek access to electronic records during their investigation of white-collar crimes. Laptop and desktop computer hard drives, system back-up tapes, pen registers, personal digital assistants and cell phones may all contain electronic records of events or communications that relate to the crimes being investigated. But, because of the ability of these devices to hold large amounts of information created over a period of time, they may also contain information about unrelated matters and records that might be protected by attorney/client or other privileges. When electronic records are seized during a search or sought by subpoena, the government may obtain access to information it did not suspect existed and has no right to see. The owners of electronic records, therefore, need to be concerned when the government seeks access to those records and be prepared to respond swiftly and carefully.

### ***Investigations by the Federal Government***

The United States Department of Justice (DOJ) has developed a procedure to protect unrelated and privileged information from being reviewed after electronic records are obtained. The DOJ appoints prosecutors and/or agents who are not otherwise assigned to the case under investigation and directs them to review all the electronic records first and identify the portions of those records that their colleagues who are handling the case should not see. These groups of reviewing prosecutors and agents are referred to as "taint teams" because their purpose is to shield the government from a defense motion to suppress electronic record evidence based on an argument that the prosecution and investigating team was "tainted" by viewing electronic records it had no right to see. See United States Department of Justice, Criminal Division, Computer Crime and Intellectual Property Section, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, § 2(B)(7) (July 2002). While this may be the best the government can do without giving up its chance to look at all the electronic records it has seized, the taint team procedure has two significant flaws.

First, the taint team procedure does not prevent the government from seeing privileged, confidential and irrelevant information that is in the electronic records; it merely changes the identity of the

government attorneys and agents who first review that information. *See, e.g., United States v. Neill*, 952 F. Supp. 834, 840-41 & n. 14 (D.D.C. 1997) (finding that a taint team review is a *per se* intentional intrusion into attorney/client privilege and stating that taint team procedures "create an appearance of unfairness.") Second, the prosecutors and agents who serve on taint teams cannot be expected to ignore evidence of other crimes they may potentially find in the electronic records they are reviewing, even if the government would not otherwise have suspected the commission of such crimes or, if it had, would not have had the right to obtain evidence of those crimes from these electronic records. The DOJ procedure provides the illusion of protection but does not solve the fundamental problem that attorneys and agents for the government are able to review information they have no right to see.

### ***Investigations by State Governments***

It does not appear that any state government has adopted a more protective procedure than the DOJ. In fact, many states try to copy the DOJ procedure, although they may have insufficient manpower to accomplish even its theoretical protections. Experience has shown that the states are no better able than the federal government to avoid using information in electronic records that they have no right to review.

### ***Responding to Subpoenas and Search Warrants***

When the government seeks access to electronic records, the owner of those records should first try to convince the government to treat them like paper records and allow the owner's attorney to go through them, before any government agent does, and remove any records that have no relevance to the investigation or that are privileged. This kind of review can be facilitated if a person is able to make his electronic records word- or phrase-searchable.

When faced with a subpoena seeking electronic records, a party should have time to review the records. The party should negotiate a narrowing of the scope of the subpoena or an extension of time before anything is provided to the government. If the government will not agree to reasonable restrictions on scope and time, the owner of the records can file a motion to quash or for a protective order, asking a judge to review the matter. A party should never turn over electronic records in response to a subpoena if he or she has not had a chance to review them.

Search and seizure warrants, on the other hand, allow the government to take records immediately and to address their use later. In this situation, a party's attorney should immediately seek assurances from the government that it will not go through the seized records before counsel has had a chance to review them and remove privileged or irrelevant information. The party's attorney should also consider the following steps:

- Suggest that the authorities make a "mirror image" (i.e., an exact duplicate in searchable form) of any computer hard drive, rather than seize the computer for off-site review. Creating mirror images minimizes disruption and avoids the possibility that reviewing information on the original hard drive will corrupt or compromise the stored data. If computers or other electronic media are seized anyway, the owner of the records should request that they be returned as soon as possible.

- Resist any attempt by the government to copy the contents of computer hard drives onto a CD-ROM or other magneto-optical disk. Copying information onto such devices does not serve any additional forensic purpose, and, because CD-ROMs and magneto-optical disks may be "write-protected" (i.e., created in read-only format), the government can use them to conduct unauthorized and overbroad searches without leaving a record that it has done so.
- Request that the government preserve all physical evidence and other information that can be used to reconstruct its searches of the seized material. Working copies of mirror images of the hard drive and audit logs will record what files were searched, when and by whom, and will indicate whether additional copies were made. This evidence can then be used to show that the government's search exceeded the scope of the warrant or was otherwise improper.

For more information, please contact:

Stephen Jonas

[stephen.jonas@haledorr.com](mailto:stephen.jonas@haledorr.com)

Robert Keefe

[robert.keefe@haledorr.com](mailto:robert.keefe@haledorr.com)