

**Steele Hansmeier** PLLC  
Intellectual Property Law Firm

October 19, 2011

38 MILLER  
AVENUE, #263  
MILL VALLEY  
CALIFORNIA,  
94941

P: 415.325.5900  
SLGIBBS@WEFIGHTPIRACY.COM

***Preservation of Evidence (Spoliation) Warning Letter to Opposing Counsel***

***Via Email (mcb@hemispheres.pro, mcb@postmodern.com)***

***Re: Case No. 4:11-cv-01566  
Client: Seth Abrahams***

Dear Mr. Berch:

**I. Demand for Preservation of Evidence**

The purpose of this letter is to confirm the obligation of your client, Mr. Samuel Teitelbaum, to take reasonable steps to preserve all documents, tangible things and electronically stored information (hereinafter "ESI") potentially relevant to any issues in the above entitled matter. Preservation means taking reasonable steps to:

1. Ensure that potentially relevant documents, tangible things and ESI are not destroyed, lost or relinquished to others, either intentionally, or inadvertently such as through the implementation of an ordinary course document retention/destruction policy;
2. Ensure that potentially relevant documents, tangible things and ESI are not modified – an issue that arises particularly in the case of ESI (which may be modified by the simple act of accessing the information), and in the case of documents used on an ongoing basis in the operation of the business; and
3. Ensure that potentially relevant documents, tangible things and ESI remain accessible – again, an issue that arises particularly in the case of ESI, which may require particular forms of software or hardware to remain readable.

Failure to comply with this notice can result in severe sanctions and penalties being imposed by the Court for spoliation of evidence or potential evidence<sup>1</sup>. To avoid such sanctions it is

<sup>1</sup> See, e.g., *Krumwiede v. Brighton Associates, LLC*, 2006 WL 1308629 (N.D. Ill. May 6, 2006). (Default judgment granted, and sanctions issued, for deleting, altering and accessing electronic data despite litigation hold);

**Exhibit D**

essential to ensure that potentially relevant materials are preserved intact and unmodified in their original form, until counsel has had an opportunity to assess the relevance of the records and the appropriate means of production of the records to opposing parties.

The obligation to preserve the relevant documents, tangible things and ESI arose when your client received notice from their ISP putting them on notice of this potential litigation.

Although we may bring a motion for an order preserving documents and things from destruction or alteration, your client's obligation to preserve documents and things for discovery in this case arises in law and equity independently from any order on such motion. Nothing in this demand for preservation should be understood to diminish your existing obligation to preserve documents, tangible things, ESI and other potentially relevant evidence.

## II. Electronically Stored Information (ESI)

Importantly, the obligation to preserve documents applies to data and information in electronic form<sup>2</sup>. The obligation extends to all ESI, stored on any kind of electronic media. The possible forms of ESI include not only emails and word processing documents, but also spreadsheets and other accounting data, the contents of databases, electronically-stored voice mail records, archived and deleted files, autorecovery files, web-based files such as internet history logs, temporary internet files and "cookies," and metadata.

ESI resides not only in areas of electronic, magnetic and optical storage media reasonably accessible to you, but also in areas you may deem not reasonably accessible. You are obliged to preserve potentially relevant evidence from both these sources of ESI, even if you do not anticipate producing such ESI.

The demand that you preserve both accessible and inaccessible ESI relevant to this matter is limited, reasonable, and necessary. As you are aware, the recent state and federal laws require that you preserve and at the appropriate time produce all sources of ESI. For good cause shown, the court may order production of the ESI, even if it finds that it is not reasonably

---

*Arista Records v. Tschirhart*, No. SA-05-CA-372-OG, 241 F.R.D. 462, 466 (W.D. Tex. Aug. 23, 2006) ("In this case, defendant's conduct shows such blatant contempt for this Court and a fundamental disregard for the judicial process that her behavior can only be adequately sanctioned with a default judgment. No lesser sanction will adequately punish this behavior and adequately deter its repetition in other cases.")

<sup>2</sup> Courts have made it clear that all information available on electronic storage media is discoverable, whether readily readable ("active") or "deleted" but recoverable. See, e.g., *Easley, McCaleb & Assocs., Inc. v. Perry*, No. E-2663 (Ga. Super. Ct. July 13, 1994) ("deleted" files on a party's computer hard drive held to be discoverable, and plaintiff's expert was allowed to retrieve all recoverable files); *Santiago v. Miles*, 121 F.R.D. 636, 640 (W.D.N. Y. 1988) (a request for "raw information in computer banks" was proper and obtainable under the discovery rules); *Gates Rubber Co. v. Bando Chemical Indus., Ltd.*, 167 F.R.D. 90, 112 (D. Colo. 1996 (mirrorimage copy of everything on a hard drive "the method which would yield the most complete and accurate results," chastising a party's expert for failing to do so); and *Northwest Airlines, Inc. v. Teamsters Local 2000, et al.*, 163 L.R.R.M. (BNA) 2460, (USDC Minn. 1999) (court ordered image-copying by Northwest's expert of home computer hard drives of employees suspected of orchestrating an illegal "sick-out" on the internet).

accessible. Accordingly, even ESI that you deem reasonably inaccessible must be preserved in the interim so as not to deprive our client of its right to secure the evidence or the Court of its right to adjudicate the issue.

Electronic documents and the storage media on which they reside contain relevant, discoverable information beyond that which may be found in printed documents. Therefore, even where a paper copy exists, we will seek all documents in their electronic form along with information about those documents contained on the media. We also will seek paper printouts of only those documents that contain unique information after they were printed out (such as paper documents containing handwriting, signatures, marginalia, drawings, annotations, highlighting and redactions) along with any paper documents for which no corresponding electronic files exist.

Adequate preservation of ESI requires more than simply refraining from efforts to destroy or dispose of such evidence. You must also intervene to prevent loss due to routine operations and employ proper techniques and protocols suited to protection of ESI. Be advised that sources of ESI are altered and erased by continued use of your computers and other devices. Booting a drive, examining its contents or running any application will irretrievably alter the evidence it contains and may constitute unlawful spoliation of evidence. Consequently, alteration and erasure may result from your failure to act diligently and responsibly to prevent loss or corruption of ESI.

### **III. Avoiding Spoliation**

You must act immediately to preserve potentially relevant ESI. Through discovery we expect to obtain from you a number of documents and things, including files stored on your client's computers and your client's computer storage media. In order to avoid spoliation, you need to preserve the data on the original media, or on exact copies of that media (sometimes referred to as image, evidentiary, or mirror copies), and be able to prove that the original matches the copy in every respect. Do not reuse any media to preserve this data.

Additionally, in order to avoid spoliation you may have to suspend certain normal computer maintenance procedure, including but not limited to such procedures as:

1. De-fragmenting hard drives;
2. Running any "disk clean-up" processes;
3. Purging the contents of e-mail repositories by age, capacity or other criteria;
4. Overwriting, erasing, destroying or discarding back up media;
5. Re-assigning, re-imaging or disposing of systems, servers, devices or media;
6. Running antivirus or other programs effecting wholesale metadata alteration;
7. Releasing or purging online storage repositories;
8. Using metadata stripper utilities;
9. Disabling server or IM logging;
10. Deleting internet cookies; and
11. Deleting browser history, bookmarks and favorites.

Our discovery requests will ask for certain data on the hard disks, floppy disks and backup media used in your client's computers, some of which data are not readily available to an ordinary computer user, such as "deleted" files and "file fragments." As you may know, although a user may "erase" or "delete" a file, all that is really erased is a reference to that file in a table on the hard disk; unless overwritten with new data, a "deleted" file can be as intact on the disk as any "active" file you would see in a directory listing.

Your client is also to preserve and not destroy all passwords, decryption procedures (including, if necessary, the software to decrypt the files); network access codes, IO names, manuals, tutorials, written instructions, decompression or reconstruction software, and any and all other information and things necessary to access, view and (if necessary) reconstruct the electronic data we will request through discovery.

You should anticipate that certain ESI, including but not limited to spreadsheets and databases, will be sought in the form or forms in which it is ordinarily maintained. Accordingly, you should preserve ESI in such native forms, and you should not select methods to preserve ESI that remove or degrade the ability to search your ESI by electronic means or make it difficult or burdensome to access or use the information efficiently in the litigation. You should additionally refrain from actions that shift ESI from reasonably accessible media and forms to less accessible media and forms if the effect of such actions is to make such ESI not reasonably accessible.

You should further anticipate the need to disclose and produce system and application metadata and act to preserve it. System metadata is information describing the history and characteristics of other ESI. This information is typically associated with tracking or managing an electronic file and often includes data reflecting a file's name, size, custodian, location and dates of creation and last modification or access. Application metadata is information automatically included or embedded in electronic files but which may not be apparent to a user, including deleted content, draft language, commentary, collaboration and distribution data and dates of creation and printing. Be advised that metadata may be overwritten or corrupted by careless handling or improper steps to preserve ESI. For electronic mail, metadata includes all header routing data and Base 64 encoded attachment data, in addition to the To, From, Subject, Received Date, CC and BCC fields.

#### **IV. Specific Requests**

Accordingly, electronic data and storage media that may be subject to our discovery requests and that your client is obligated to maintain and not alter or destroy, include but are not limited to the following:

- 1. Computers:** The following steps should immediately be taken to safeguard all computers.
  - a. **Computer:** Your client is not to destroy or modify any computers used or potentially used in the downloading of the copyrighted content at issue in this case. This includes, but is not limited to:

- i. Desktop computers, laptops, home computers, personal digital assistants, cell phones, Blackberrys, Palm Pilots or similar multi-functional devices, voicemail, digital cameras, other digital storage devices such as floppy disks, CD's, DVD's, zip drives, backup media, external hard drives and USB ("thumb") drives.
    - ii. Any components attached to or contained within the computers such as the hard drive, tape drive, computer bus, CPU, motherboard, RAM, storage controllers, media devices, modem, router, and monitor.
    - iii. Relevant electronic information, such as data files contained within those computers. This includes relevant electronic information stored on your client's behalf by third parties such as banks, professionals (such as accountants or lawyers), the government, insurers, third party service providers, affiliated companies, data warehouses or internet service providers.
  - b. Fixed drives attached to such computers: (i) a true and correct copy is to be made of all electronic data on such fixed drives relating to this matter, including all active files and completely restored versions of all deleted electronic files and file fragments; (ii) full directory listings (including hidden files) for all directories and subdirectories (including hidden directories) on such fixed drives should be written; and (iii) such copies and listings are to be preserved until this matter reaches its final resolution.
  - c. All floppy diskettes, CDs, magnetic tapes and cartridges, and other media used in connection with such computers prior to the date of delivery of this letter containing any electronic data relating to this matter are to be collected and put into storage for the duration of this lawsuit.
2. **The Copyrighted Content at Issue:** With regard to the copyrighted data file: Your client is not to modify or delete any data files, "deleted" files and file fragments related to the copyrighted content at issue in this case existing at the time of this letter's delivery, which meet the definitions set forth in this letter, unless a true and correct copy of each such electronic data file has been made and steps have been taken to assure that such a copy will be preserved and accessible for purposes of this litigation.
3. **Networking Equipment:** With regard to any networking equipment: Your client is not to modify or delete any equipment used to connect to any network associated with your client's IP address relevant to this case. This includes, but is not limited to any modems and routers associated used or potentially used to connect to the network associated with said IP address.
4. **Programs Used to Download the Copyrighted Material:** With regard to any programs used or that could potentially have been used to download to the relevant

copyrighted content: Your client is not to modify or delete such programs. This includes, but is not limited to, any BitTorrent software or programs, used in any manner by your client, not just to download the copyrighted material.

5. **Access to Relevant Websites:** With regard to any websites where the relevant copyrighted material was found and downloaded by your client: Your client is not to modify or delete anything related to accessing these websites. This includes, but is not limited to, deleting internet cookies, deleting browser history, bookmarks and favorites.
6. **Online Data Storage on Mainframes and Minicomputers:** With regard to online storage and/or direct access storage devices attached to your client's mainframe computers and/or minicomputers: Your client is not to modify or delete any electronic data files, "deleted" files and file fragments existing at the time of this letter's delivery, which meet the definitions set forth in this letter, unless a true and correct copy of each such electronic data file has been made and steps have been taken to assure that such a copy will be preserved and accessible for purposes of this litigation.
7. **Offline Data Storage, Backups and Archives, Floppy Diskettes, Tapes and Other Removable Electronic Media:** With regard to all electronic media used for offline storage, including magnetic tapes and cartridges and other media that, at the time of this letter's delivery, contained any electronic: Your client is to stop any activity that may result in the loss of such electronic data, including rotation, destruction, overwriting and/or erasure of such media in whole or in part. This request is intended to cover all removable electronic media used for data storage in connection with their computer systems, including magnetic tapes and cartridges, magneto-optical disks, floppy diskettes and all other media, whether used with personal computers, minicomputers or mainframes or other computers, and whether containing backup and/or archive data sets and other electronic data, for all of the computer systems.
8. **Replacement of Data Storage Devices:** Your client is not to dispose of any electronic data storage devices and/or media that may be replaced due to failure and/or upgrade and/or other reasons that may contain electronic data.
9. **Fixed Drives on Stand-Alone Personal Computers and Network Workstations:** With regard to electronic data which existed on fixed drives attached to stand-alone microcomputers and/or network workstations at the time of this letter's delivery: Your client is not to alter or erase such electronic data, and not to perform other procedures (such as data compression and disk de-fragmentation or optimization routines) that may impact such data, unless a true and correct copy has been made of such active files and of completely restored versions of such deleted electronic files and file fragments, copies have been made of all directory listings (including hidden files) for all directories and subdirectories containing such files, and arrangements have been made to preserve copies during the pendency of this litigation.

- 10. Programs and Utilities:** Your client is to preserve copies of all application programs and utilities, which may be used to process electronic data covered by this letter.
- 11. Log of System Modifications:** Your client is to maintain an activity log to document modifications made to any electronic data processing system that may affect the system's capability to process any electronic data regardless of whether such modifications were made the client and/or any other third parties.
- 12. Evidence Created Subsequent to This Letter:** With regard to electronic data created subsequent to the date of delivery of this letter, relevant evidence is not be destroyed and your client is to take whatever steps are appropriate to avoid destruction of evidence.

#### **V. What We Want You to Do**

In order to assure that your obligation and your client's obligation to preserve documents and things will be met, we request you do the following:

1. Forward a copy of this letter to your client and all other persons and entities with custodial responsibility for the items referred to in this letter;
2. Provide Plaintiff with a copy of any correspondence you have sent or will send to your client regarding the preservation of all documents, tangible things and ESI potentially relevant to any issues in this matter;
3. With respect to Blackberry or similar multi-functional devices, voicemail, digital cameras and USB drives, please ensure that those devices (and in particular the devices of the above named individuals/employees) are immediately imaged by an IT department or professional. Since these devices often have limited memory, any delay may result in relevant ESI being destroyed. We also require confirmation of the dates when those devices are captured and imaged;
4. Preserve any log or logs of network use, whether kept in paper or electronic form, and to preserve all copies of your backup tapes and the software necessary to reconstruct the data on those tapes, so that there can be made a complete, bit-by-bit "mirror" evidentiary image copy of the storage media of each and every personal computer (and/or workstation) and network server in your control and custody, as well as image copies of all hard drives retained by you and no longer in service, but in use at any time from to the present;
5. Provide Plaintiff with a letter containing the following information:
  - a. Confirmation that your client is aware of his obligations explained above.
  - b. The steps taken so far by your client to preserve the relevant documents, tangible things and ESI referenced above;

- c. Provide a catalog of any spoliation, destruction, or modifications to any relevant documents, tangible things and ESI that has already occurred, either intentionally or unintentionally; and
  - d. Any measures taken to remedy the spoliation that has already occurred to any relevant documents, tangible things and ESI.
6. Provide Plaintiff with further letters cataloging and explaining any further spoliation that takes in the future with an explanation on what remedial measures have taken place to reduce or eliminate the harm caused by the spoliation.

We would welcome the opportunity to speak with you to discuss the scope of production of all documents, including the searching and production of ESI. We ask that you contact us to discuss, among other things, the appropriate search parameters for all electronic records in this matter.

We thank you in advance for your anticipated co-operation.

Sincerely,



Brett L. Gibbs, Esq.

BLG/gfy

E

Prenda Law Inc. | 305-748-2102

wefightpiracy.com/litigation.php | Other bookmarks

Home | About Us | Contact Us | Recent Sampling of Cases filed

## Welcome

Prenda Law is a law firm that provides legal services to content producers and creative professionals. Our focus is pursuing individual and business owners who infringe on the copyrights created with our clients creative works. Our practice includes utilizing the unique legal aspects of Internet based piracy where the defendant's infringement occurs under the cover of Internet Protocol (IP) addresses. In addition, our firm pursued the servers that host our clients' pay websites to steal digital content. Prenda Law actually prosecuted the litigation.

### Prendas Top 25 Pirates (Individual Cases)

<p>Case 1:12-cv-00001-Prenda-Law Inc. v. [Name]</p> <p>Case 1:12-cv-00002-Prenda-Law Inc. v. [Name]</p> <p>Case 1:12-cv-00003-Prenda-Law Inc. v. [Name]</p> <p>Case 1:12-cv-00004-Prenda-Law Inc. v. [Name]</p> <p>Case 1:12-cv-00005-Prenda-Law Inc. v. [Name]</p> <p>Case 1:12-cv-00006-Prenda-Law Inc. v. [Name]</p> <p>Case 1:12-cv-00007-Prenda-Law Inc. v. [Name]</p> <p>Case 1:12-cv-00008-Prenda-Law Inc. v. [Name]</p> <p>Case 1:12-cv-00009-Prenda-Law Inc. v. [Name]</p> <p>Case 1:12-cv-00010-Prenda-Law Inc. v. [Name]</p> <p>Case 1:12-cv-00011-Prenda-Law Inc. v. [Name]</p> <p>Case 1:12-cv-00012-Prenda-Law Inc. v. [Name]</p> <p>Case 1:12-cv-00013-Prenda-Law Inc. v. [Name]</p> <p>Case 1:12-cv-00014-Prenda-Law Inc. v. [Name]</p> <p>Case 1:12-cv-00015-Prenda-Law Inc. v. [Name]</p> <p>Case 1:12-cv-00016-Prenda-Law Inc. v. [Name]</p> <p>Case 1:12-cv-00017-Prenda-Law Inc. v. [Name]</p> <p>Case 1:12-cv-00018-Prenda-Law Inc. v. [Name]</p> <p>Case 1:12-cv-00019-Prenda-Law Inc. v. [Name]</p> <p>Case 1:12-cv-00020-Prenda-Law Inc. v. [Name]</p> <p>Case 1:12-cv-00021-Prenda-Law Inc. v. [Name]</p> <p>Case 1:12-cv-00022-Prenda-Law Inc. v. [Name]</p> <p>Case 1:12-cv-00023-Prenda-Law Inc. v. [Name]</p> <p>Case 1:12-cv-00024-Prenda-Law Inc. v. [Name]</p> <p>Case 1:12-cv-00025-Prenda-Law Inc. v. [Name]</p>	<h3>Links</h3> <ul style="list-style-type: none"> <li>Home</li> <li>About Us</li> <li>Contact Us</li> <li>Recent Sampling of Cases filed</li> </ul> <h3>Resources</h3> <ul style="list-style-type: none"> <li>Copyright Law</li> <li>DMCA</li> <li>Internet Piracy</li> <li>Prenda Law</li> </ul>
---	---

Understand, we are unable to list and provide the link to any and currently pending the without the courts due to some limitations. However, our firm will be providing a sampling of individual cases that we file each month.

1:00 PM 2/28/2012

Exhibit E

For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now.

Other bookmarks

Home About Us Contact Us

Recent Sampling of Cases filed

3005-18-2102

### Welcome

People Law is a law firm that provides cost-effective and efficient legal services to individual practitioners, law firms, and corporate clients. We are currently accepting applications for attorneys and paralegals. For more information, please contact us at (800) 555-1234. We are currently accepting applications for attorneys and paralegals. For more information, please contact us at (800) 555-1234.

### Prondas Top Pirates (Individual Cases)

Links  
Resources

Pronda Law Firm, LLC  
10000 E. 1st Avenue, Suite 1000  
Denver, CO 80231  
Phone: (303) 733-1234  
Fax: (303) 733-1235  
Email: info@prondalaw.com

12:35 PM  
1/12/2012