

EXHIBIT B

From: Pozza, Duane
Sent: Friday, February 11, 2011 4:20 PM
To: Janet Munn
Cc: Fabrizio, Steven B; Platzer, Luke C; Gabriel Nieto; Felix Rodriguez
Subject: Disney Enterprises, Inc. v. Hotfile Corp.

Janet,

I am following up on our discussions and correspondence over the last three days regarding the plaintiffs' anticipated motion for expedited discovery and a preservation order, including your discussion with Steve Fabrizio earlier today. We have repeatedly explained the relief that we are seeking and the bases for seeking it, noting the risk of evidentiary spoliation in this case. As noted below, defendants have not been willing to agree to meaningful relief that will ensure that critical relevant is preserved. I include below a list of the categories of data that plaintiffs are seeking to have preserved but that defendants have not agreed to preserve.

As we have explained, in the normal course of defendants' operation of Hotfile, defendants must receive and maintain different kinds of data that will be central evidence in this case. In the course of today's discussion, defendants have agreed to preserve certain data that defendants maintain in their ordinary course of business: User IDs, URLs of content files, numbers of downloads of content files, content file size, and content file uploader IP addresses. Defendants have also suggested that content files deleted by users are currently preserved for 20 days, and that defendants will suspend deletion of those files, though only if plaintiffs share in the cost of storage.

These proposals would not provide meaningful relief against the risk of spoliation. Defendants have not agreed to stipulated entry of a court order to preserve such data, nor have they agreed to preserve other relevant data that plaintiffs have identified. However, all relevant data must be preserved, including a number of categories of data that plaintiffs have identified to you:

- (1) All data regarding Hotfile users, whether registered or unregistered, including records of uploads or download by users.
- (2) All content files. It is defendants' obligation to preserve all such files, which constitute direct evidence of infringement. Further, as we have noted, Hotfile appears to have a policy of routinely deleting at least some files that have not been accessed for a period of time, which must also be suspended.
- (3) All additional content reference data regarding such content files, which may include additional data such as file name and download by country.
- (4) All records of payments to users or third-party link site operators under any of Hotfile's "Affiliate" programs, including all data that Hotfile uses to determine those payments, and all records identifying those users or third-party link sites.
- (5) All business and marketing plans related to defendants' businesses.
- (6) All communications regarding Hotfile, including records of communications with registered users and other website operators via any email address used by defendants.
- (7) All internal communications between and among defendants and their employees regarding defendants' businesses.
- (8) Any data regarding use of Hotfile or communications with Hotfile that are maintained by third parties at the direction of Hotfile.

Further, defendants have not agreed to our request for expedited discovery of (a) content reference data identifying or regarding the content files stored on Hotfile's servers and downloads of such files, and (b) a sample of content files. As we have explained to you, this expedited discovery is appropriate not only given the spoliation risk, but because it will help manage your clients' preservation obligations. Once we obtain the content reference data, we will be able to specify a subset of content files for expeditious production. This will allow us to obtain critical evidence of infringement quickly, at which point we would stipulate that Hotfile could modify its preservation of all content files, even as to those that would be deleted in the ordinary course. This procedure will in fact relieve any burden of preserving content files.

Defendants also have not agreed to our request for immediate Doe discovery into the identity of any other person or entity involved in the operation of Hotfile, any person or entity operating a third party website paid for directing user traffic to Hotfile including via Hotfile's "Affiliate" program for third-party website operators, and the persons or entities with the greatest amounts of payments under Hotfile's "Affiliate" program for uploaders.

Finally, we remind you that defendants have an obligation to preserve *all* relevant data that Hotfile receives and uses in the normal course of operation, including download requests that will include information such as IP address of the requesting user, the URL requested, and the time of request. Any retention policy by which that data is deleted must be suspended, and that data must be preserved electronically, such as by enabling logging functionalities to store such data. *See, e.g., Columbia Pictures Indus., Inc. v. Bunnell*, 245 F.R.D. 443 (C.D. Cal. 2007).

Regards,
Duane

Duane Pozza

Jenner & Block LLP
1099 New York Avenue, N.W.
Suite 900
Washington, DC 20001-4412
Tel (202) 639-6027
Fax (202) 661-4962
DPozza@jenner.com
www.jenner.com

CONFIDENTIALITY WARNING: This email may contain privileged or confidential information and is for the sole use of the intended recipient(s). Any unauthorized use or disclosure of this communication is prohibited. If you believe that you have received this email in error, please notify the sender immediately and delete it from your system.
