EXHIBIT A

The evidence demonstrates that Cyberheat initiated the transmission of hundreds of unsolicited commercial email messages that violated CAN-SPAM and the Adult Labeling Rule; therefore, Cyberheat should be found liable for violating the law.[5] Cyberheat reached consumers through an affiliate program called "Topbucks." As discussed below, virtually anyone could sign up as a Cyberheat affiliate through this program, and then advertise Cyberheat's websites. Cyberheat paid affiliates for bringing paying customers to Cyberheat. (Statement of Facts ("SOF") 5-10) The affiliates were the spammers who sent the violative email, but Cyberheat is responsible because it initiated the email.

Cyberheat readily acknowledges that it operated the Topbucks affiliate program. The operation of Topbucks is detailed in the Statement of Facts. (SOF 17, 18) There is similarly no dispute that email promoting Cyberheat's websites was delivered to various recipients. The government's sources of such email are twofold. First, the government received email that was gathered by Microsoft. These email messages were delivered to email accounts associated with no active person, called "trap accounts," that Microsoft set up to monitor spam activity over the Internet. (SOF 65, 66) The other source of violative email the government relies upon is an FTC-maintained database which contains emails that members of the public forwarded to an FTC maintained address, "spam@uce.gov." This is called the "spam database." (SOF 85) Email that was delivered to these two sources promoting Cyberheat websites is associated with various Topbucks affiliates. (SOF 65-105) The government does not anticipate that Defendant will seriously dispute any of this. Rather, the government believes that Cyberheat will dispute its legal liability for violative email associated with its (or sent by) Topbucks affiliates.

David Vetter is a Program Manager for MSN Hotmail, which is part of Microsoft Corporation. Mr. Vetter's declaration, attached as Exhibit 2, describes why Microsoft is

---

[5] The effective date of CAN-SPAM is January 1, 2004, and the effective date of the Adult Labeling Rule is May 19, 2004. The violative emails initiated by Cyberheat after January 1, 2004, and before May 19, 2004, only violate the CAN-SPAM Act as the Rule was not effective when the emails were initiated. References in the Memorandum to email violating both the Act and the Rule refer to those email messages sent on or after May 19, 2004.

concerned with the phenomenon of spam, and describes the "Hotmail trap accounts" that Microsoft has created to determine whether incoming email complies with Microsoft policies. Mr. Vetter states that Microsoft has not consented to anyone to send email to the trap accounts. (Ex. 2, p. 2; SOF 65) He also states that Microsoft, through its counsel, provided to the government copies of certain email that was received by the Hotmail trap accounts. (Id.; SOF 66)

Chad R. Bundy is an attorney who represents Microsoft Corporation in certain matters related to spam. Mr. Bundy's declaration, attached as Exhibit 3, describes email in a database Microsoft created which contains email received in the Hotmail trap accounts that Mr. Vetter discussed in his declaration. Mr. Bundy's declaration details the manner in which he provided the government with copies of email from the Hotmail trap accounts. He states that the email was provided to the government in specific formats and that he also provided certain "web captures" that allow a viewer to view the web page to which some of the email was linked. (Ex. 3, SOF 66)

Allyson Himelfarb, an Investigator with the Federal Trade Commission, reviewed the emails obtained through the trap accounts and spam database. Her declaration, attached as Exhibit 1, details how these emails violate CAN-SPAM and the Rule and explains how these emails are associated with specific Cyberheat affiliates.

The emails from Microsoft and the spam database that the government alleges violate CAN-SPAM and the Adult Labeling Rule are attached to the Himelfarb declaration on a CD-ROM readable by computer. (Government Ex. 30, described in Himelfarb declaration, ¶ 7.[6]) Ms. Himelfarb describes the format of the emails that Microsoft

[6] Government Ex. 30 contains the universe of email messages that the United States contends violate CAN-SPAM and the Adult Labeling Rule. Government Ex. 31 contains images of the specific email messages discussed in Ms. Himelfarb's declaration, which the declaration refers to as copies of printouts with specific attachment numbers. The page after Ms. Himelfarb's declaration further explains the contents of Government Ex. 31. The specific email messages from Government Ex. 31 discussed in Ms. Himelfarb's declaration are attached as hard copies to the courtesy copy of exhibits provided to chambers.

provided or which came from the spam database, and the web captures that she conducted related to some emails received from Microsoft. (Ex. 1, ¶¶ 5-6) She states that she reviewed hundreds of emails from ten Cyberheat affiliates (id., ¶ 7), and much of the balance of her declaration details specific emails associated with those affiliates.

After explaining how each email or group of emails is related to Cyberheat, the declaration typically states that the email failed to include the required label ("SEXUALLY-EXPLICIT:") in the subject line or initially viewable area, did contain sexually-explicit material within the initially-viewable area, failed to include a valid physical postal address for Cyberheat, and contained an opt-out mechanism (if at all) only after the sexually-explicit material rather than within the initially-viewable area of the message. (Himelfarb declaration, ¶¶ 12, 13, 14, 15, 18, 22, 23, 24, 28, 29, 30, 31, 32, 33, 37, 39, 41, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 57, 59) Each of these emails is an exhibit to the Himelfarb declaration. Each contains sexually-explicit material in the initially viewable area which CAN-SPAM and the Adult Labeling Rule forbid, as alleged in Count I. Further, each email fails to contain matter required by CAN-SPAM and the Adult Labeling Rule as alleged in Count I, and each email fails to contain matter required by CAN-SPAM as alleged in Counts II and III of the Complaint.

A. Cyberheat's Websites Were Promoted via Unsolicited Commercial Email Messages that Contain Sexually Oriented Material

Cyberheat affiliates promoted Cyberheat's websites through unsolicited commercial email messages that contained sexually oriented material. The hundreds of email messages at issue were "unsolicited." Many of the email messages were delivered to the Microsoft trap accounts, which were dummy accounts set up just to see what spam would be delivered to them. These accounts received violative email simply because they existed. Microsoft never provided consent to anyone to send spam to any of the trap accounts. (SOF 65, 104) The United States sought from Cyberheat any evidence it had regarding affirmative consent to "receive commercial electronic mail message[s] containing sexually oriented material." Cyberheat produced no responsive documents.