EVAN A. SCHMUTZ (3860)
eschmutz@hjslaw.com
WM. KELLY NASH (4888)
wmkellynash@aol.com
JORDAN K. CAMERON (12051)
jcameron@hjslaw.com
HILL, JOHNSON & SCHMUTZ, L.C.
River View Plaza, Suite 300
4844 North 300 West
Provo, Utah 84604
Telephone: (801) 375-6600
Fax: (801) 375-3865

Attorneys for Plaintiff Zoobuh, Inc.

UNITED STATES DISTRICT COURT
DISTRICT OF UTAH, CENTRAL DIVISION

ZOOBUH, INC., a Utah Corporation Plaintiff, vs. BETTER BROADCASTING, LLC., a Utah limited liability company; IONO INTERACTIVE, a company doing business in Utah; DOES 1-40 Defendants.	**LETTER OF OPINION OF F. ALAN FULLMER** Case No.: 2:11cv00516-DB Judge David O. Nuffer

May 28, 2012

Letter of Opinion
F. Alan Fullmer

I have prepared this written opinion at the request of ZooBuh, Inc. for use in its litigation against Better Broadcasting, LLC and IONO Interactive.

I. FACTS OR DATA CONSIDERED IN FORMING THE OPINIONS STATED BELOW

1. All electronic mail messages received by ZooBuh's mail servers that are at issue in this litigation.
2. 15 U.S.C. 7701 *et seq.* (the CAN-SPAM Act).
3. National Cyber Alert System, Cyber Security Tip ST04-007.
4. *Recognizing and Avoiding Email Scams,* US-CERT
5. *Technical and Policy Requirements for Sending Email to AOL,* AOL Postmaster

II. EXPERTISE/EXPERIENCE

I have been in the computer field for over 30 years. I have been directly involved in email communication systems and infrastructure since 1996. I have created proprietary email systems specifically to facilitate alternative services such as customized filtering and implementation and modification of open-source products. I have configured and maintained various Mail Transfer Agent ("MTA") mailers such as Microsoft Exchange, Qmail and Postfix. I have extensive knowledge of Spamassassin, which is a popular anti-SPAM tool that interfaces with many types of MTAs. I have also developed various email filtering programs that interface with Postfix, PHP and MySQL.

My knowledge of networks and network protocols along with my knowledge of server management and maintenance qualifies me as an expert in this field.

III. SCOPE OF OPINION

I was asked to opine regarding the following topics: History of Email Communication; Technology of Email Communication; Email Safety Practices and Standards; Common Spamming Practices; Better Broadcasting's Email Practices.

I am not being paid for the work that I do on behalf of the Plaintiff in this case.

IV. OPINION

HISTORY OF EMAIL COMMUNICATION

1. Electronic mail (E-Mail) was originally designed for 7-bit American Standard Code for Information Interchange ("ASCII") text only. ASCII is a character scheme based on the US English alphabet. The letters include upper and lower case alphabet, numbers and

symbols found on a typical US computer keyboard. Since email predates the inception of the Internet, a text only format was used. These emails were sent as early as the 1970s.

2. Hyper Text Markup Language ("HTML") did not come about until the early 1990s. HTML allows a message to specify font families, sizes, colors, and to have italic, underline or bold letters.

3. Over time, the need to send attached files became necessary, thus resulting in a process we now know as Multipurpose Internet Mail Extensions ("MIME"). MIME enabled the use of extended character sets and the ability to encode binary data (e.g., attachments) with the use of base64. Base64 converts binary data into an ASCII/text-only alternative in order to transmit the email and have it be decoded by the recipient's email client.

4. Most modern graphical email clients can display either plain text or HTML for the message body, usually at the option of the recipient. Although HTML emails can include a text copy, it is not required for the successful transmission of email.

5. There are advantages of using HTML such as font sizes, colors, italics, underlines and bold text. However, some disadvantages include increased size of the email, and more importantly, privacy concerns such as image tracking, web bugs, and phishing schemes.

TECHNOLOGY OF EMAIL COMMUNICATION

6. There are three components to an email; the Envelope, Header, and Body. The Envelope is not relevant for this opinion. The Header and Body are the two parts of email relevant to this opinion.

EMAIL HEADER

7. In simple terms, the Header is the first part of the message. (an example of a Header is attached here to as **Exhibit "A"**). It is not displayed to the user by default. However any email client will allow the recipient to view the full header.

8. The Header includes several identifying lines such as "From", "To, cc", "Date", "Subject."

9. The "From" includes the sender's email address and optionally the sender's name. This lets the recipient know who sent the message. There is no real check on this name and it can be set to any data by the emailer. If there is no "return-to" header and/or if the recipient does not exist on the receiving system, the server will look at the "From" line to bounce the message back. Falsified addresses will bounce back to bad address and can play "ping-pong" (depending on configurations) between the two servers, thereby causing harm to the servers.

10. The "To, Cc" identifies the recipient's email address and name. Multiple addresses are separated by commas. Bcc addresses will not be shown as they are "Blind Carbon Copies." Each recipient email address will be in one of these fields.

11. The "Date" is set by the sender's email client. The date is typically not checked for accuracy, however, SPAM checkers such as Spamassassin can determine if it was sent in the future or in the past (day old bread) based on the attached time zone in the RFC2822[1] date.

12. The "Subject" line provides a summary of the content of the email, but can contain any information input by the sender.

[1] RFC standards discussed in more detail below.

13. The Header also includes routing lines that indicate when and where the email was handled, and by what server. It is time stamped by the Mail Transfer Agent ("MTA") indicating that the message routed, or relayed off the server.

14. Emails can take different routes, bouncing and relaying off different servers to arrive at the intended destination. MTA servers facilitate these transfers. Each time the email relays off a server, a "Received" tag is added to the Header.

15. The Header can facilitate custom fields as well including, but not limited to, the "Hostname" and "IP Address" of the various mail servers along with "Date Stamps", "SPF Reports" (used for a SPAM analysis), "SPAM Summaries", etc.

Headers are crucial in determining the origination and tracking path of the message.

16. The Header has distinct roles related to the identification of the initiating party (the party who transmitted the email message) that are completely unrelated to what may or may not exist in the email Body.

17. For example, each header contains a received line designed for debugging/tracing the path of the message and for tracking down slow relays that affect deliverability. The received lines can serve as three main components in a review of where the message has been:

a. first, it can identify where the message originated from and if the server is authorized to handle distribution of the domain;
b. second, it identifies the receiving/destination server—the last server to handle the data; and
c. third, it can be used to chart the path of the message—each server, in between, that has relayed or forwarded the message.

18. The "From" line in each message may include a designated sender name and always includes an originating email address. This information is set by the emailer and can be forged and/or falsified without any trouble. There is no verification of its validity, so steps such as SPF records (utilized by SPAM filters to identify offending email) were created to try and combat the false information.

19. The recipient mail server does initial evaluations based on the Header information to determine the legitimacy of the sending server. The server will examine the information in an attempt to identify whether the message is legitimate or some sort of attack. SPAM filters will take the analysis a step further and identify specific characteristics and information in order to determine if the email is SPAM.

20. When a Header contains false information, the recipient mail server is unable to identify the actual source of the message, or will identify the source as something other than what it actually is (i.e. a "spoof"), thereby preventing the mail server, the protected computer, and/or the end recipient from identifying the actual point of origination.

21. Further, as a practical matter, the Header serves as a way whereby the recipient can identify the sender and origin without opening the email and potentially exposing the recipient to questionable content and/or potentially exposing the recipient computer to security threats (i.e. viruses, Trojans, malware, etc.).

EMAIL BODY

22. The body of an email message can be drafted as text only, HTML, or both by using the MIME protocol.

Text Only Emails

23. Email bodies can be drafted as text only and are 7 bit ASCII. Text emails are "plain text", which means there is no formatting, such as fonts, sizes, colors. Every email client, even one with the most strict security settings, should be capable of reading text emails.

24. Email clients that are only capable of reading text, or email clients that are only configured to read text, will not read and display HTML. (*See infra*).

25. Text emails are the smallest form of email and the easiest for a receiving mail client to process. This fact is commonly known in the industry.

HTML Emails

26. The body of an email messages can also be drafted as HTML. HTML allows a message to specify font families, sizes, colors, and to have italic, underline or bold letters.

27. An email has to specify to the email client that it is using an alternative/additional format (i.e. MIME, discussed *infra*), otherwise the email client will display the message as plain text and will look like you "viewed the source" of a webpage, which will be illegible to the recipient. (an example of this is provided herewith as **Exhibit "B")**.

28. Email clients that are configured to read HTML will also read and display text, as HTML capable email clients are capable of reading and displaying simple text.

29. In contrast, an email message that only includes an HTML part will only be read by an email client that is both capable of reading HTML and configured to read HTML. This is because email clients that are only capable of reading text, or email clients that are only configured to read text, will not read and display HTML. This fact is commonly known in the industry.

MIME Emails

30. MIME is an Internet standard that extends the format of email to support message bodies with multiple parts. MIME is specified in six linked RFC memoranda: RFC 2045, RFC 2046, RFC 2047, RFC 4288, RFC 4289 and RFC 2049.[2]

[2] In order for computer to computer communication to work, standards are created and maintained. The RFC protocols together define email specifications for all Internet users. The Internet Engineering Task Force ("IETF") codifies standardizing decisions which are then published in Request for Comments ("RFC"). Many RFCs are the standards on which the Internet is formed. By way of example, the Internet Email RFC standards include: RFC 2049, which defines a message representation protocol specifying considerable detail about US-ASCII message headers, and leaves the message content, or message body, as flat US-ASCII text. This set of documents, collectively called the MIME, redefines the format of messages to allow for: (1) textual message bodies in character sets other than US-ASCII; (2) an extensible set of different formats for non-textual message bodies; (3) multi-part message bodies, and (4) textual header information in character sets other than US-ASCII.

31. Since MIME extends the format of email to support message bodies with multiple parts, MIME allows email to be drafted in a manner that the email can be read in more than one format. For example, using the MIME protocol, an email can be drafted to have a text part, a HTML part, or both. MIME also allows the emailer to include images as part of the message.

32. There are three main types of images that can be included within an email: "Attached"; "Inline"; and "Remote."

33. Attached: images (and other files) can be attached to a message which typically requires the end-user to click on an icon to open them up to view or download.

34. Inline Attached: these types of images are inline with the content of the body. They can either be positioned on the page with text flowing around, or just sequentially one after another. The image data is part of the email, encoded with base64, and referenced with a content ID ("CID#"). A common purpose of this method is to have an article, newspaper, magazine type content within the email.

35. Remote: these images are not part of the email body, but rather a link to a web server that could be anywhere on the Internet and controlled by any unknown third party. Many email clients, such as Outlook, ZooBuh, and Google, will warn the user that there is remote content and require the user to click and accept before the images are downloaded. This is a standard security measure. Remote images are considered a security threat because they require additional connections from the recipient's computer to an offsite server. The images also allow a recipient to be tracked if the image is viewed.

36. Remote images are not permanent. If the remote image no longer exists on the remote server (the file was moved, deleted, etc. by the third party in control of the server) then the image will not be downloaded to the email client and can never be viewed by the recipient.

37. Remotely hosted images typically do not have a very long shelf-life. This means there is a small window of time where the image is viewable. There are many reasons for this, including but not limited to: (1) the emailer violated the Terms and Conditions of the ISP (i.e., spamming. Most ISPs policies include provisions against spamming, such as Moniker, GoDaddy, Name Cheap, Network Solutions, etc.); (2) the allocated bandwidth amount has been exceeded (when an emailer sets up a remote server with a hosting company, there is usually a bandwidth limit set. When a spam campaign is initiated, hundreds of millions of emails may be sent out. Each recipient that opens the image(s) counts against this bandwidth. If the bandwidth is exceeded, the image will no longer be available to subsequent viewers); (3) The file has been deleted or removed (there are many reasons this may happen. Whatever the case, the image will no longer be available on the server and the recipient will never be able to view it).

Summary

38. An email message sent in MIME with only a text part should be displayed by legitimate email clients. This is because email clients that are configured to read HTML will also read and display text, as HTML capable email clients are capable of reading and displaying simple text.

39. In contrast, an email message that only includes an HTML part will only be read by an email client that is both capable of reading HTML and configured to read HTML. This is because email clients that are only capable of reading text, or email clients that are only configured to read text, will not read and display HTML.

40. If an email is drafted using the MIME protocol to include both a text part and an HTML part, the email will be readable as a text message or as rendered HTML. However, if the email is drafted to only have an HTML part, then anyone who receives the email who is not set up to read HTML messages will not be able to read the email.

41. Thus, anyone who sends a multi-part message using the MIME protocol and does not include the text version of the email should expect that the recipient may not be able to see the content included in the email. Indeed, when an email is drafted in HTML format, many email clients are configured to warn the author of an email that the recipient may not be able to read the message as a result of the HTML format.

42. The result of the choice to send emails where the content is HTML or remotely hosted is that any recipient of the email who uses an email client that is not capable of rendering HTML code will not be able to see any information in the HTML part of the email body. This is a fact that is commonly known in the industry.

43. Additionally, any recipient of the email who has an email client capable of rendering HTML code but who has turned that functionality off (whether for preference or because of potential security threats) will also not be able to see any of the content provided in the HTML part of the email body.

GENERAL EMAIL SAFETY PRACTICES FOR EMAIL RECIPIENTS

44. The United States Department of Homeland Security (DHS) through the United States Computer Emergency Readiness Team ("**US-CERT**") is charged with providing response support and defense against cyber attacks for the Federal Civil Executive Branch and with information sharing and collaboration with state and local government, industry and international partners.

45. US-CERT interacts with federal agencies, industry, the research community, state and local governments, and others to disseminate reasoned and actionable cyber security information to the public.

46. US-CERT has repeatedly warned against downloading remotely hosted images in email.

47. In the National Cyber Alert System, Cyber Security Tip ST04-007, US-CERT advised as follows: "Disable the automatic downloading of graphics in HTML mail – *Many spammers send HTML mail with a linked graphic file that is then used to track who opens the mail message—when your mail client downloads the graphic from their web server, they know you've opened the message.* Disabling HTML mail entirely and viewing messages in plaint text also prevents this problem." (National Cyber Alert System, Cyber Security Tip ST04-007, 2, attached hereto as **Exhibit "C"**).

48. If the spammer knows the email has been opened, they have confirmed the legitimacy of the email address, as most spam is directed towards dictionary lists. The spammer then has the ability to distribute the email address as a confirmed address which makes it more valuable.

49. In the document entitled *Recognizing and Avoiding Email Scams*, US-Cert again warns "[t]here are a number of ways you can configure your email client to make you less susceptible to email scams. For instance, configuring your email program to view email as 'text only' will help protect you from scams that misuse HTML in email." (*Recognizing and Avoiding Email* Scams, 8, attached hereto as **Exhibit "D"**).

50. Industry also warns of rendering HTML in email messages. In the document entitled *Technical and Policy Requirements for Sending Email to AOL*, AOL warns emailers that they will not support many of the features of HTML. (*See Technical and Policy Requirements for Sending Email to AOL*, attached hereto as **Exhibit "E"**).

51. AOL also states that "[o]ne reason [the client does not support all features of HTML] is because of the security hazards involved with sending HTML e-mails. These e-mails can expose the unwary user to hostile viruses or other intrusive programs. . . . The common theme here is end-user security. Malicious e-mailers can bury a wide variety of harmful actions within the HTML e-mail, including programs that activate upon download." *Id*. at 2-3.

COMMON SPAMMING PRACTICES

52. Spammers engage in various practices designed to (1) conceal the actual sender from the recipient (2) avoid SPAM filtering technology; (3) induce the recipient to open the email; (4) track the recipient email address and verify its validity; and (5) potentially harm the recipient or the recipient's computer.

53. Spammer will use generic emails address and "From" names in the email Headers. Email spammers will often use false names and email addresses, sometimes randomly generated, so the recipient will not know who really sent the email. Further, using false and generic names will often evade spam filters designed to identify know spammer "From" names and email addresses.

54. Spammers will register hundreds, if not thousands, of ".info" domain names from which to send countless email. The ".info" domains are considerable cheaper than ".net", ".com", or ".org" domains. At the time of this writing, GoDaddy is registering ".info" domains for $2.99 USD or free if purchased with a ".com" domain name. In contrast, ".com" names cost $12.99 USD, ".net" names cost $9.99 USD, and ".org" names cost $6.99 USD. In the likely event that the domain used in the "From" line gets blacklisted or suspended, the messages have already been sent out and at minimal investment. Further, spammers generally do not have any intention of renewing a ".info" domain as it would be more expensive than obtaining new names. Further, after a spam campaign, a domain is likely blacklisted and the receipt of the message by the recipient would be blocked. Also, new names benefit the spammer as the name is new and has not been blacklisted in RBL (Registered Black List) lookups.

55. Spammers will set fake "dates" in the emails. Email spammers often attempt to set this date in an effort to place the email at the top of the recipient's inbox, as most email clients sort by date.

56. Spammers will use "Subject" lines to induce the recipient into opening the email. Common practices include: identifying the recipient by name; stating that the recipient is a winner or has obtained something for free; using the "re" or "fwd" designations to make the recipient believe the email is a response or coming from a trusted emailer.

57. Spammers use remotely hosted images to track and confirm legitimate email addresses. A common use of a Remote Image would be: where the "abc123" is a unique identifier that is associated with the recipient's email address. If the recipient were to open the message and view the image, the spammer would be able to confirm that the email address is authentic. Additionally, it is very common for email spammers to include, in remotely hosted images, the language that identifies the ability to unsubscribe from future messages, an advertisement notice,

or the identification of contact information for the emailer. Concealing the content from the recipient in a remote image often times prevents the recipient from unsubscribing from future messages or successfully identifying the emailer.

58. Spammers use "Bayes Poisoning" to evade SPAM filters. Bayesian filtering in SPAM is a method to help determine if a message is SPAM. It uses tokens or words, comparing with legitimate messages, to calculate a probability that an email is or is not SPAM. When using HTML to send messages, it allows for comment lines. Comment lines are encapsulated with <!-- and -->. Anything within these tags is not viewable by the email recipient. However, the SPAM filter does see it. When the SPAM filter scans through the document, it finds hundreds or thousands of random words included in comment lines with the sole purpose of confusing or poisoning the Bayesian filter. The objective is to make the filter think that the message is legitimate by outweighing real words with known spamming words, in an attempt to throw off the ratio. (*see infra* Exhibit H).

59. Spammers use Dictionary Attacks to generate and discover legitimate email addresses. A Dictionary Attack is a process where a spammer attempts to successfully target an exhaustive list of pre-arranged values. A Dictionary Attack does not indicate words from the typical book such as Webster's Dictionary, but information on particular subjects or on a particular class of words, names, or facts, usually arranged alphabetically. Although Dictionary Attacks are notably used for attempting passwords, they are also used for usernames in email addresses.

60. Spammers use scripting or other automated processes to discover legitimate email addresses ("**Scripting Attacks**"). A Scripting Attack is where email addresses (either sender or recipient) are generated using an automated process. The result is a list of sender or recipient email addresses that follow various patterns (e.g. John1@email.com to John9999@email.com). Often times, scripting processes are more sophisticated and instead of using lists, they use words. Viewing the email addresses alphabetically will reveal a pattern of selected words. In some cases, the words will cross various domain names, indicating the same script generated words for multiple domains.

BETTER BROADCASTING'S EMAIL PRACTICES

61. I have reviewed each of the emails in question. Each of the Better Broadcasting emails is designed using HTML or the MIME Protocol.

62. The emails in question are capable of including text, HTML, attached, in-line and remotely hosted images.

63. Each of the emails contains various remotely hosted images. However, text only clients, and clients with security settings that prevent the automatic download of remote images or the rendering of HTML (which is an industry standard practice) will never display this content.

64. Furthermore, the images in the emails appear to have had a short shelf-life and no longer exist on the remotely hosted server. Even clients that are able to view HTML in its entirety would get an "image not found" type of message, or the iconic "X in the box" replacement. Accordingly, the recipient would never see the content of the image.

65. Though the emails provide content in the text part of the email. The emails fail to include any of the content or information required by the CAN-SPAM Act (i.e. advertisement notice, unsubscribe notice, physical address of sender) in this format.

66. The emails contain many common spamming practices.

a. Generic email addresses. Almost all (13,333) of the emails in question originated from generic or nonsensical email addresses and do not actually identify any party. (list of email addresses attached hereto as **Exhibit "F"**).

b. High concentration of ".info" sender domains. (list of all sender domains attached hereto as **Exhibit "G"**). The Better Broadcasting emails in this case originated from 13,289 unique sender email addresses. 11,778of these addresses are ".info" addresses. Given the high number of ".info" addresses, it is my opinion that Better Broadcasting registered each of the domains for spamming purposes only.

c. Each email contains the following remotely hosted image: <img src="http://gaiana.jiggly-joggly.info/uMu/1001" border="0">. The sub-domain "gaiana" can separate groups within the jiggly-joggly.info domain. Such as geographic location, master lists (where the email was purchased from or obtained), recipient addresses and can be used for purposes of confirming the validity of a recipient email address.

d. Bayes Poisoning. A significant number of the Better Broadcasting emails (approximately 60%) also contain significant "Bayes Poisoning." (Email sample of Bayes Poisoning, attached hereto as **Exhibit "H"**). The Bayes Poisoning is so severe that, in the case of some of the emails, a printed raw version (a version which displays all text, including hidden white text) would span over 900 printed pages.

e. Script Attacks. The sender email addresses from which the Better Broadcasting emails were sent appear to have been generated by some sort of script based on a selection of words. In this case, most of the sender email addresses do not contain an individual's, company's or brand's name, but a random and generic word or nonsensical letter combination. (*see* Exhibit F). Viewing the sender email addresses alphabetically shows a distinct pattern of selected words. Some words cross domain names, indicating the same script generated words for multiple domains, essentially using the same dictionary file to create these sender email addresses.

CONCLUSION

67. Though the MIME protocol allows Better Broadcasting to provide a text version of the email content, which would be viewable by any recipient, most, if not all, of the messages from Better Broadcasting, have only one line of text that is readable without the use of remotely hosted images.

68. As stated above, most, if not all, of the emails utilize remotely hosted images to provide content to the Body of the email. Again Better Broadcasting should expect that recipients who use text only email clients, who have security setting that block HTML, or who have security settings that block the automatic download of remotely hosted images (which is industry standard) will never see the content of the remotely hosted images. Further, if the remote images are removed from the server for any reason, which seems to be the case here, the recipient will never see the content.

69. In my opinion, the only way to ensure that the recipient will actually see the content of the email Body is by providing it in text. This would not significantly increase the

size of the message and would not prohibit the emailer from also providing more attractive advertisements in images or HTML. It would, however, ensure that every recipient sees the content.

70. In summary, Better Broadcasting should expect that any recipient who uses a text only email client, or any recipient who has security settings that block HTML or remotely hosted content (industry standard), would not be able to see the content in the email Body.

F. Alan Fullmer