New York Law Journal
Technology Today

VOLUME 234—NO. 122 TUESDAY, DECEMBER 27, 2005 ALM

The Information Trail

Litigators Use E-Mail Headers to Trace Origins of Messages

BY MARK A. BERMAN AND AARON ZERYKIER

ELECTRONIC DISCOVERY

Mark A. Berman

Aaron Zerykier

A benefit of having e-mails produced in electronic form is that it permits a litigator to follow the "information trail" contained in the imbedded "header"[1] of an e-mail that would otherwise be unavailable from the printed copy of the e-mail.[2]

This "header" information may be used to identify the Internet account from which the e-mail was sent because the header often includes the Internet protocol (IP) address assigned to the user who sent the e-mail.

Determining the identity of the unknown or anonymous person that sent a specific e-mail can be critical in various types of litigations, including defamation and tortuous interference cases, as well as in cases where a person is utilizing an e-mail address "confusingly" similar to a company's address in order to, inter alia, commit fraud or to unfairly compete.

Internet service providers (ISPs), such as America Online, Verizon DSL, or Road Runner, utilize certain ranges of IP addresses. The ISP assigns a specific IP address to each service subscriber, usually on a session by session basis, when a subscriber connects to the Internet.[3]

The specific IP address, in addition to the date and time the e-mail was sent, may be used to identify the owner of the account from which the e-mail was sent.

In *Matter of the Application of TD Waterhouse Group, Inc.*, Index No. 1005020/05 (N.Y. Sup. Ct. Feb. 14, 2005), for example, TD Waterhouse, the brokerage company, was granted pre-action disclosure from Time Warner Cable, pursuant to CPLR §3102(c), to determine the owner of two e-mail addresses so TD Waterhouse would be able to assert an action for, inter alia, fraud, trademark infringement, false designation of origin and unfair competition.

Today's litigator must not only know what electronic information he needs to obtain through the discovery process, but also how to use such information to his maximum advantage.

In *TD Waterhouse*, the e-mails in question were apparently part of a scam to utilize the brokerage's name in soliciting bank cashing services.

The fraudulent header, however, provided no information that would permit TD Waterhouse to identify its origination, and the only identifying feature of the e-mail was that responses were to be sent to e-mail accounts that ended with "@austin.rr.com."

A forensic investigator employed by TD Waterhouse used the services of a Web site called SamSpade.org to determine that the ISP who provided the austin.rr.com e-mail addresses was Road Runner, which is owned and operated by Time Warner Cable.

The court granted TD Waterhouse's CPLR §3102(c) application and directed that Time Warner Cable provide the identity of the persons and/or entities who were registered to use or had access to the inbox for the subject e-mail accounts; copies of any e-mails that contained or referred to the tradename TD Waterhouse; records reflecting traffic in the offending e-mail accounts; the content and source of replies to the offending e-mails; the nature and identity of any information, including, any header information or links to other information sites that were contained in the offending e-mails; and such other information that may be related to the identity of any person using the subject e-mails.

'Anonymous' Messages

IP address information embedded in e-mails may also reveal the identity of the author of an allegedly defamatory "anonymous" e-mail.

In *Schubert v. American Express Co.*, 4/18/01 N.Y.L.J. 18 (col. 2) (N.Y. Sup. Ct. Mar. 30, 2001), petitioner sought pre-action discovery in order to commence a defamation action. The allegedly defamatory e-mail was sent from a Yahoo.com address. The petitioner had previously been granted discovery against Mindspring, the ISP the sender used to send the e-mail.

In support of his application, petitioner submitted an affidavit from a forensic computer expert who averred that he had traced the origination of the e-mail by

Mark A. Berman *is a partner of Ganfer & Shore.* **Aaron Zerykier** *is an associate at the firm.*

researching the information contained in the e-mail's header. The offending message originated from Yahoo.com, and the expert indicated he was able to ascertain the specific IP address from which the e-mail was sent because Yahoo imbeds the IP address of the user into the header of each e-mail sent with its service.

The expert was able to utilize a computer program "which converts the IP addresses to names and vice versa" and was thus able to ascertain that the IP address in question was owned by Mindspring.com.

Mindspring had produced documents that indicated the sender's account had been opened using a fictitious name, but Mindspring documents disclosed the American Express account number used to pay the ISP. Petitioner was thus granted discovery from American Express of the name and address of the credit card owner who had paid for the Mindspring account.[4] See *The Public Relations Society of America, Inc. v. Road Runner High Speed Online*, 8 Misc. 3d 820, 799 N.Y.S.2d 847 (N.Y. Sup. Ct. 2005) (pre-action discovery granted, on default, in a putative defamation case; Road Runner was directed to produce all documents concerning a certain IP address and all documents in its custody or control relating to a particular e-mail[5]); *In the Matter of the Application of Bayerische Landesbank*, Index No. 102237/05 (N.Y. Sup. Ct. March 22, 2005) (pre-action subpoenas and depositions granted, on default, to determine: the name and address of the person responsible for creating and using a certain e-mail address, what other e-mails were sent from such e-mail address, and the name and address of all persons or entities involved with the creation and use of the fraudulent and misleading e-mail address); *Hart v. America Online, Inc.*, Index No. 110850 (N.Y. Sup. Ct. Aug. 23, 2004) (pre-action discovery granted, on default, in a putative defamation and injunction case.)

IP address information may also be used to help determine the identity of a user that has allegedly hacked into a corporate network or has posted defamatory statements on a message board.

In *Workstream, Inc. v. Cablevision Systems, Corp.*, Index No. 15034/04 (N.Y. Sup. Ct. April 9, 2004), the court required the production of "all information including account records, in [Cablevision's] possession concerning" a specific IP address, which petitioner "identified as the computer used by the person or persons who utilized Cablevision as his or her Internet Service Provider to hack into the computer database of Workstream and illegally access its confidential and proprietary business information." See also *In the Matter of KPMG Consulting, Inc.*, Index No. 015483/02 (N.Y. Sup. Ct. Sept. 26, 2002) (requiring the production of "all documents mentioning or in any way concerning the identity of the holders and/or users" of a specific IP address which was utilized to post information on an internet message board).

Maximum Advantage

Today's litigator must not only know what electronic information he needs to obtain through the discovery process, but also how to use such information to his maximum advantage.

The above techniques that were used to support applications for pre-action discovery can also be used to analyze the origin of an e-mail produced during a litigation. For example, in intellectual property or trade secret litigations, the name of the sender of an e-mail from an Internet-based e-mail account might reveal the identity of the person who may have solicited the purchase or sale of offending merchandise or sought proprietary company information.

When making an application to a court seeking discovery of the identity of an Internet user from an ISP, a computer expert should be consulted, and sworn documentary evidence and/or oral testimony should be provided in support of any such application.

Expert affidavits should be specific, in the description of the techniques used by the expert to identify the ISP, as well as the date and time the subject user was connected to the Internet through the ISP.

Moreover, as many of the above types of applications are granted on default, a petitioner should be clear and precise as to the specific discovery needed, as the court may well grant the exact relief requested.

Conclusion

In sum, as demonstrated above, while a sender of an e-mail might think that his identity had been disguised, this may not always be true.

E-mails may be traced back to the sender through information maintained by the user's ISP.

The mechanisms for tracing an e-mail, however, are not fool-proof, and a savvy user may seek to avoid his or her identity being discovered by, inter alia, accessing an Internet-based e-mail account from a public ISP (such as the free wireless internet connections provided in a number of parks in New York City); "piggybacking" onto an unsecured wireless network; providing an ISP with false identification or paying for the ISP's services with a stolen credit card. Nonetheless, where determining the origin of an e-mail is important, tools exist to provide for such identification.

1. Through most e-mail programs, it is possible to view an e-mail's header. For example, to view header information in Microsoft Outlook, a user clicks on View and then selects Options.

2. See "Forensic Inspection of Computer Hard Drives Under New York Law," Sept. 1, 2005, NYLJ, and "Are Private E-Mails Really Private?", Oct. 7, 2005.

3. A discussion of IP addresses and their history can be found in the decision entitled *Name.Space, Inc. v. Network Solutions, Inc.*, 202 F.3d 573 (2d Cir. 2000).

4. The putative sender of the e-mail, "John Doe," was granted intervenor status to oppose petitioner's application, and the sender's motion to dismiss, as well his request for a hearing to determine the actual origination of the e-mail, was denied. The court found John Doe's alleged expert affidavit to be conclusory, without a supporting factual basis, and inconsistent. The court also noted that John Doe did not submit an affidavit "denying involvement or knowledge" of the subject e-mail.

5. The "John Doe" sender of the e-mail sought to intervene and to quash the requested discovery on the grounds that, inter alia, the statements made in the e-mail in question were covered by the First Amendment. The court held that John Doe had "no legitimate reasonable expectation of privacy for his internet account information" nor did he "present[] any other valid basis for preserving his anonymity."

Ganfer & Shore, LLP
360 Lexington Avenue
New York, New York
212.922.9250
MBerman@ganshore.com