Searching For John Doe: Finding Spammers and Phishers

Aaron E. Kornblum
Internet Safety Enforcement Attorney
Legal & Corporate Affairs
Microsoft Corporation
Redmond, WA 98052-6399
(425) 705-3210
aaronko@microsoft.com

Abstract

Microsoft has prosecuted a vigorous civil enforcement campaign against spammers and phishers. When initial investigation into a spam or phishing case fails to reveal the identity of the person(s) responsible, filing a "John Doe" lawsuit and following up with thorough third-party discovery has been an effective strategy to unmask the perpetrator.

1 Meeting John Doe

Spammers employ a variety of deceptive and fraudulent techniques to obfuscate their true identity. Such techniques include: forging email header data such as the From: and Reply-To: lines; using open proxies and/or infected zombie computers to retransmit mail; and registering beneficiary websites with false data or stolen credit card information. Consequently, it can be challenging for a spam recipient – whether an individual consumer or a sophisticated ISP investigator – to determine with certainty that a particular spammer was responsible for sending an illegal e-mail. This is significant because traditional legal enforcement mechanisms (such as a lawsuit) generally require specific identification of an opposing party, or defendant.

Enter John Doe. In most jurisdictions, an aggrieved person may file a "John Doe" complaint against a defendant whose identity is not known while trying to determine the defendant's actual name. Doe suits may be used in a variety of circumstances.[1] After filing a Doe suit, a plaintiff can seek court permission to issue subpoenas – formal written orders commanding a person to appear under penalty – under the rules of evidentiary procedure. Once the court grants such authorization, a plaintiff can unilaterally serve subpoenas on third-parties that may possess information concerning the true identity of the defendant(s). Subpoena recipients – such as ISPs, payment processors, and website hosting companies – generally are required to respond to the subpoena with the data sought by the plaintiff. Upon receiving the subpoena responses and, where possible, identifying a culpable party, the plaintiff can amend its complaint to reflect the correct name of the defendant(s) and then pursue its claims.

2 Microsoft v. John Doe

In early 2003, Microsoft commenced its ongoing enforcement campaign against spammers. To date, the company has initiated 106 civil actions in U.S. courts against spam defendants, as reflected in some further detail below.

Table 1: Microsoft Spam Lawsuits

No. of Lawsuits	How Lawsuit Was Initiated
43	Against Named Defendants
63	Against "John Doe" Defendants

Further, on March 31, 2005, Microsoft filed 117 additional civil actions in federal court in Seattle against phishing defendants. All of these actions were initiated against "John Doe" Defendants.

[1] John Doe suits have been used in many legal realms, including automobile accidents, securities law, privacy and civil rights. Doe suits also may be employed in a reverse manner to shield the name of the plaintiff. For example, plaintiff Norma McCorvey used the pseudonym "Jane Roe" to challenge abortion laws in *Roe v. Wade*. *See* 410 U.S. 113, 120 n.4 (1973).

3 Lessons Learned

Microsoft's experience filing John Doe spam and phishing lawsuits has been extremely positive. Microsoft investigations in Doe lawsuits typically begin by focusing on the owner of a website advertised in illegal spam. In order to learn more about such a website owner, Microsoft issues subpoenas to entities holding key information about the owner, including: domain registrars, e-mail service providers, Internet Service Providers, web hosts, financial institutions, and payment processors.

To date, in its spam enforcement cases Microsoft has issued 837 civil subpoenas to third parties, as reflected in some further detail below:

Table 2: Most-Frequently Subpoenaed Third Parties

No. of Subpoenas	Third Party
41	PayPal, Inc.
40	Yahoo, Inc.
29	Network Solutions
27	eNom, Inc.
24	Intercosmos

On average, third parties have responded to subpoenas issued in Microsoft spam cases in 29 days from the date of the subpoena issuance.

As a part of its 117 filed phishing cases, Microsoft to date has issued 34 civil subpoenas to 18 third parties.

3.1 Evidence Obtained Via John Doe Subpoena

Domain registrars possess several pieces of important customer data including: a registrant's credit card number used to pay for services; a valid e-mail address used for administrative purposes; and a list of domains paid for with the same credit card or owned by the same account holder. A subpoena to a registrar can reveal all of this information, as well as commonly a history of communications between the registrar and the account holder, updates to the WHOIS records for the domains at issue, and records of spam complaints concerning the advertised domains. Similarly, web hosting records can be subpoenaed to learn who is paying for hosting services for a website at issue.

Once a registrant's e-mail address is confirmed, it is then possible to subpoena the e-mail service provider to obtain account registration and billing information, as well as a history of the IP addresses used to log in to the account. At that point, it also is possible to subpoena the IP address owner (the ISP) to obtain records identifying the subscriber assigned to the IP address used to access the account in question.

Of course, there is no guarantee that such account and subscriber information is accurate and there is nothing to prevent an individual from providing false information to, for example, an ISP. In fact, information received in discovery from service providers and financial institutions sometimes reveals a case of identity theft where the credit card account owner has been victimized. Similarly, the temporal nature of such information can cause challenges. Case prosecutions have been more successful where subpoenaed third parties retained detailed customer records and information.

Another aspect of Microsoft's subpoena investigative strategy is to follow the money trail left by cybercriminals. Online payment processors such as PayPal frequently are utilized by spammers and their associates. Such processors retain detailed records of inbound and outbound transaction amounts, payee and payor e-mail addresses, and text narratives for payments, all of which may be obtained via subpoena. These records also may include product shipping addresses, IP addresses used to access the account, verified credit card and financial institution account information, and detailed notes identifying individual payments such as "1 month [web] hosting 30 days".

3.2 Success with John Doe Lawsuits

Of Microsoft's 63 suits initiated with "John Doe" complaints, 32 (51%) have been amended to identify the defendant(s) in the case based upon information obtained via subpoena. However, this percentage is skewed lower due to the fact that the third-party discovery process requires time to develop after the case is filed, and Microsoft regularly is filing new cases. In addition, Microsoft successfully has tracked and stopped a phisher using a John Doe lawsuit and the subpoena process enabled thereafter. In September and October of 2003, an unknown person launched a phishing attack seeking credit card information from MSN customers. Microsoft filed a Doe lawsuit in the U.S. District Court for the Western District of Washington. Three sets of subpoenas led Microsoft to an individual in Austria who possessed information regarding the identity of the phisher. Although the individual in Austria was not able to identify the phisher, he was able to provide to the Microsoft European legal team an additional U.S. lead (a Qwest IP address). Following a subpoena to Qwest, Microsoft ultimately identified the phisher: Mr. Jayson Harris, 21, of Davenport, IA. Microsoft referred the case to the FBI, which seized Mr. Harris' computer in July 2004 and is investigating. The MSN Billing case was reviewed in detail in a Newsweek article entitled "How to Hook the Elusive Phisher," available at:

http://www.msnbc.msn.com/id/6919230/site/newsweek/