Subpoenas, Forensic Exams and Cyber Investigation: How to Identify Anonymous or Unknown Internet Posters

Related Professionals

Whitney C. Gibson

CLIENT ALERT | 9.29.2014

It is no secret that people are more comfortable publishing harmful statements on the internet when their identities are masked. As such, the sources of internet defamation and other online reputation attacks typically publish damaging content anonymously or pseudonymously.

Therefore, pursuing an attacker in an internet defamation case often involves unmasking someone's identity. This can be accomplished in a number of ways, including through cyber investigation techniques, forensic exams, and subpoenas.

Cyber investigation

Oftentimes, consulting with a cyber investigator is an excellent and cost-efficient method of identifying unknown bad actors on the internet. Cyber investigators can successfully obtain internet protocol (IP) addresses of unknown posters which, in turn, can be used to issue subpoenas to internet service providers (ISPs) for subscriber information.

A primary technique cyber investigators often use is "pretexting." This involves misrepresenting their identity to attempt to persuade the author of a harmful post to take some action in order to obtain that author's IP address. Thus, if a harmed party is also working with an attorney, that attorney must ensure the cyber investigator is not creating ethical problems.

Forensic exams

Another very effective, but perhaps underutilized, option for determining the identity of an online attacker is to conduct a forensic exam of the suspected attacker's computer. When a victim believes he or she knows who is behind the online attack, there are often circumstantial facts and perhaps evidence that may point to the person behind the posting.

In these situations, a forensic exam can be invaluable. When conducting these exams, we often find that the attackers will have attempted to cover their tracks by deleting computer data. This may accomplished using wiping software after they received notice of the forensic exam.

In some cases, it may be possible to find "fragments" related to the deleted data, which could provide information regarding: 1) when a file was installed; 2) whether a file was modified and when; 3) when a file was deleted; and 4) information about the data contained within the file.

In short, when there is circumstantial evidence that suggests someone is the source of an anonymous or pseudonymous attack, a forensic exam is a very strong tool to prove his or her identity.

Subpoenas

Of course, as internet defamation attorneys, we regularly issue subpoenas for the production of documents containing identifying information.

Before issuing a subpoena, however, certain elements must be satisfied. The actual requirements vary by jurisdiction. But, in general, you must have a valid legal cause of action and be able to present evidence to support it.

Perhaps the most popular and followed standard is the "*Dendrite* test," although other popular tests include *Krinsky* and *Cahill*. In the New Jersey case *Dendrite Int'l Inc. v. Doe No. 3*, plaintiffs must do the following:

1. Attempt to provide notice to the anonymous defendants that their identities are being sought, and explain how to present a defense;
2. Quote verbatim the allegedly actionable online speech;
3. Allege all elements of the cause of action;
4. Present evidence supporting the claim of violation; and
5. Prove to the court the right to identify the speaker outweighs the First Amendment right of anonymous free speech

When the appropriate test is satisfied, an attorney can go forward with issuing a subpoena to the website or company hosting the damaging content.

In short, issuing subpoenas in a "John Doe" case – noting that once an unknown person's identity can be determined, he or she can be named in the lawsuit – is often a three-step process.

First, as mentioned, a subpoena can be issued to a third party website/host for identifying information. If the subpoena complies with the non-party's subpoena standards and there is no objection from the user or poster, they will produce certain information.

Often times, there is little information retrieved because the unknown person intentionally tried to hide his or her identity with limited or sometimes false information provided upon account registration. Nonetheless, a subpoena typically yields, at minimum, an IP address. Thus, the second step is determining

to which ISP the IP address is registered, which can generally be accomplished in an online search.

Once an ISP is identified, the third step involves issuing a subpoena to that ISP for the account holder information (based on the IP address used at the particular date and time the relevant online posting was made).

This three-step approach is a simplied version of what is not usually a simple process. Nevertheless, it should provide a brief overview of how an attorney can go about identifying a person who has defamed or otherwise attacked a client's reputation online. For a more-detailed version of the subpoena process, download our "Subpoena Guide for Identifying Anonymous Internet Posters."

For more information, contact Whitney Gibson at 855.542.9192 or wcgibson@vorys.com. Read more about the practice at http://www.defamationremovalattorneys.com/.