TECHNOLOGY LAW

Internet Attacks: How to Protect Your Clients' Reputations

BY GAVIN P. LENTZ AND JASON P. LISI
Special to the Legal

There has been a substantial increase in Internet-based attacks launched prior to and during litigation. These are designed to either obtain leverage in a lawsuit or harm a competitor. To avoid detection, the attackers commonly use fake Facebook pages and anonymous e-mail accounts. Unfortunately, these types of accounts can be set up without providing a correct name, address, credit card or other verifiable information — factors that encourage this type of activity.

This article will address both the legal and technical steps you should take when a client is subject to Internet-based activity that damages the client's personal or business reputation. When these Internet attacks are launched anonymously, efforts to protect your client's reputation and remove the websites promptly may be complicated, but they are not impossible.

Consider this scenario: You receive a call from a frantic client who has been harmed by false and malicious e-mails or websites — containing false and malicious statements — purporting to come from his own company or employees, as well as links to other harmful web pages.

When faced with this situation, it is critical that you, as counsel, are aware of the most expeditious methods of removing such anonymous attacks and identifying the offending parties. Otherwise, your client may sustain such significant economic harm that the outcome of the litigation may be moot. Your clients will also want you to remove the offending negative material from a basic Google search after the host site takes the material down, as it will continue to appear in search results without further action.

Below are the approaches that have worked best for our clients in these time-sensitive situations.

STEPS TO DISABLE INTERNET ATTACKS

• **Identify the offender or host of the offending site by doing a quick search on www.whois.net.** This free website will usually identify the host of a website and provide the Internet Protocol, or IP, address of the party posting the material. If you have a sophisticated party trying to conceal his or her identity, you may need the assistance of a computer specialist to do "reverse e-mail" searches or other forensic analyses to identify the wrongdoer. At trial, if you show a malicious attack was submitted anonymously by the defendant to harm your client, this will help destroy their credibility and may support an award of punitive damages and counsel fees for outrageous conduct under 42 Pa.C.S. Section 2503.

• **File an Internet complaint form using the specific forms available on each offending site.** Be advised that a threatening letter or even a draft lawsuit from a lawyer without all of the data required on the host site's complaint form will be ignored in almost all cases. Facebook, Twitter and Google all have specific complaint forms that you must use. Otherwise, they will not respond to your request no matter how urgent it is.

You should be mindful that submitting the form alone will not work immediately unless you are aggressive in following up with the host site's legal department after you have submitted the complaint form. Only after the form has been filed can you threaten to sue the hosting site unless they remove the material. This is because the hosting sites such as Google are not liable under the Digital Millennium Copyright Act (DMCA) unless they are on actual notice that the material on their site is being posted unlawfully. You will need to identify information that is demonstrably false or malicious if you want to pursue a cause of action for defamation.

You can also threaten the website or hosting party with liability after they are put on written or electronic notice by counsel of the false information that is being publicized on their site and thereafter, if they refuse to remove it.

It is critical that you, as counsel, are aware of the most expeditious methods of removing anonymous online attacks and identifying the offending parties.

Depending on the facts, you could also assert a [illegible] action for invasion of privacy under the *Restatement of Torts Second* — even if the information is not actually false, but casts your client in a false light and is presented in a way that harms your client — for example, posting misleading or untruthful information on Facebook and surreptitiously distributing it to all of your client's friends. Wrongdoers can get away with this by setting up fake Facebook pages and tricking your clients into "friending" them under the false belief that they are connected to your client or their business.

• **Another option is to assert copyright or trademark claims covering any of the information being used that will provide an additional basis to pressure the hosting site to take the information down promptly.** While hosting sites are normally not liable simply for posting the information, once they are put on notice that they are hosting copyrighted or trademarked material without your client's authorization, they can also be sued for damages. This type of threat usually does the trick, but only if you follow up with their legal department with multiple calls, faxes, and e-mails after you also assert all of this in a Complaint Form. Otherwise, it could take months for sites such as Google or Facebook to take any action. In the meantime, your client's reputation is being harmed on a daily basis.

LENTZ LISI

GAVIN P. LENTZ *is a partner in Bochetto & Lentz in Philadelphia.*

JASON P. LISI *is the founder and principal of Legal Internet Solutions Incorporated, a website development and search engine marketing company for law firms.*

• **Issuing a subpoena without filing a formal lawsuit.** This can be done without filing a formal complaint to [illegible] and continue your efforts to identify the offenders though other means fail. There are essentially two procedures for doing this, depending on the facts. In Pennsylvania, you can simply file a writ of summons and seek to take depositions and [illegible] Pennsylvania Rule of Civil Procedure 4008. This rule permits depositions and service of a subpoena to obtain documents needed to discover the relevant facts to draft a complaint in a lawsuit. (We have found that many Internet hosts will actually respond and provide documents if you simply fax a copy of a subpoena to their legal department.) This process becomes more difficult if the hosting company is located in another state. For example, Yahoo is located in California and usually will not provide any documents unless you also obtain an order for the court in Pennsylvania ordering an out-of-state deposition or subpoena. This process can take several days but the Internet provider will ultimately provide you with the available information.

Another method of issuing a subpoena anywhere in the United States without filing a complaint is under the DMCA. If you can assert that any aspect of what the offending parties are using is copyrightable material you may issue a subpoena in any federal district in the United States. (Note: It is possible to file a copyright registration electronically in one day covering material your client developed, including the appearance of a web page and then immediately proceed under DMCA even before you have received the final copyright registration.) The benefit of this process is that you are in federal court and able to issue a subpoena in any state. See 17 USC [illegible]

• File a request for temporary restraining order (TRO) if the less expensive methods [illegible] above [illegible]

Technology Law continues on 7