

continued from page 7 >>

OBTAINING AN ANONYMOUS INTERNET SPEAKER'S IDENTITY

While the First Amendment shields Claude's right to anonymity, defamation is never protected speech. T&C can therefore obtain Claude's identity by requesting a court order compelling disclosure — though this may not be as simple as it sounds. T&C must show: (1) Claude received adequate notice and reasonable opportunity to respond; (2) its claim could survive a summary judgment motion; and (3) balancing the parties' interests favors disclosure.

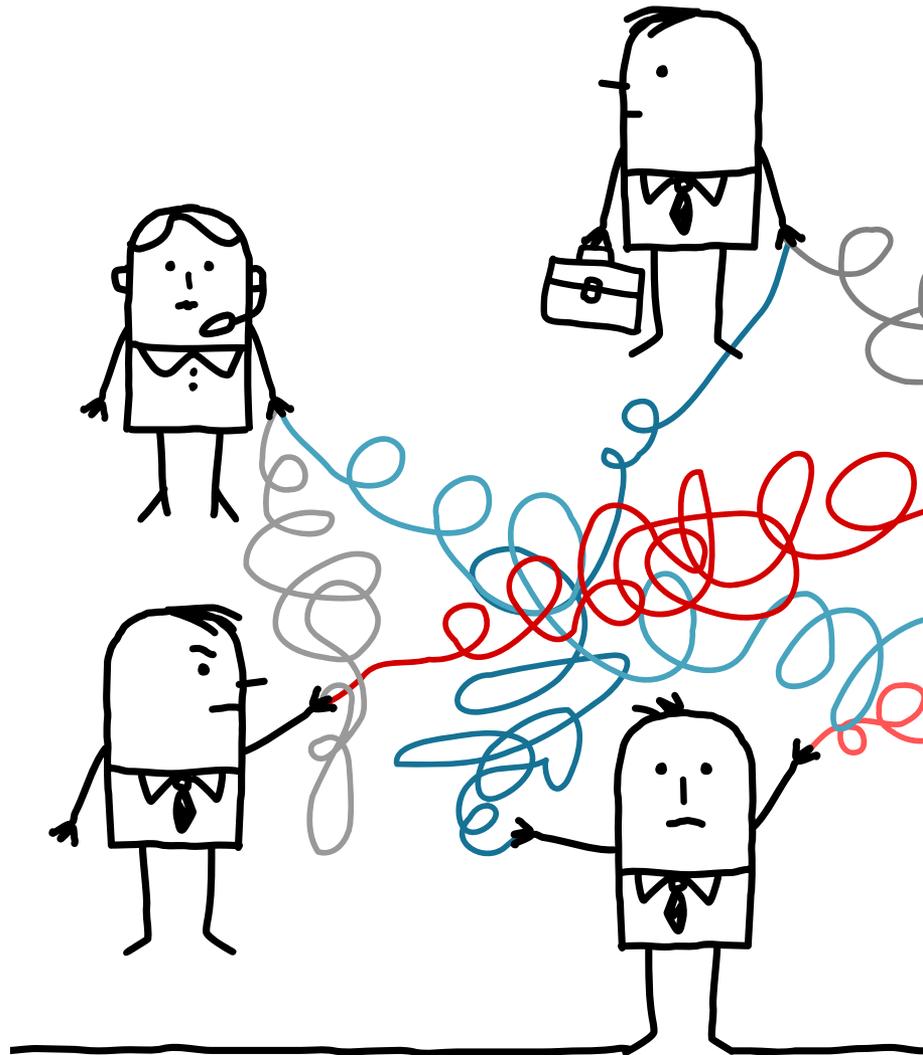
Directly responding to a defamatory statement generally satisfies the first element. For example, T&C could simply reply to the website postings and wait a reasonable time for Claude to respond. To meet the second element, T&C must show a genuine issue of material fact exists, such as whether the statements were actually defamatory. Lastly, because defamation is not protected speech, T&C's inability to proceed with its case likely outweighs Claude's loss of anonymity.

INJUNCTIVE RELIEF

T&C could obtain supplemental relief by requesting an injunction. This may be necessary if Claude refuses to cooperate with T&C's requests for identification of the author. If granted, the court could order Claude to remove the defamatory postings and enjoin him from making similar statements in the future.

CONCLUSION

In summary, the law views interactive computer service providers, such as complaint and review websites, as the "town square," and the town is not liable for what individual members of the public say in the town square, no matter how defamatory. The key to obtaining relief for Internet defamation is identifying and pursuing claims under traditional defamation theories against the author of the statement.



SO YOU WANT TO SUBPOENA YOUR ADVERSARY'S GMAIL, FACEBOOK POSTINGS, AND TEXT MESSAGES ...

BY WILLIAM M. FISCHBACH

E-mail and text messages are undoubtedly the preferred method of communication in today's business environment. Consequently, civil discovery often focuses on the retention and acquisition of these electronic communications. One party typically propounds a discovery request to its opposing party requesting the production of all relevant e-mails within a certain time frame, and the other party responds. The concern that often arises is whether the party responding to the request has provided every relevant electronic communication in the party's possession. The old Russian proverb *doveryai no proveryai* — "trust but verify" — would seem to apply. So how to verify?

When a party sends and receives e-mail in Microsoft Outlook or a similar application, she will likely maintain and have access to her own private e-mail server. In that instance, someone can typically image the data on the e-mail server to obtain relevant e-mails. A

SO YOU WANT TO SEE YOUR ADVERSARY'S PHONE RECORDS ...

BY ASHLEY N. ZIMMERMAN

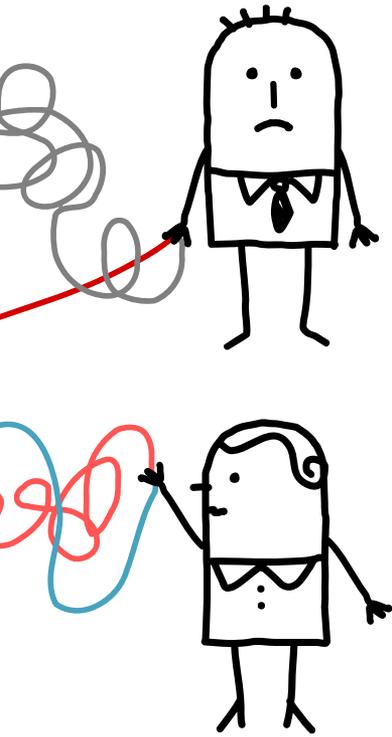
In addition to the restrictions imposed on the disclosure of cellular phone records by the Stored Communications Act ("SCA"), 18 U.S.C. § 2701, *et seq.*, cellular phone companies maintain disclosure and retention policies for data on their users.

Much like subpoenas to e-mail hosts, subpoenas to cellular phone companies must be directed to the company's dedicated subpoena division, and include user information such as the user's name, telephone number, Internet Protocol (IP) address, date and time of connection, and in some instances, time zone. Additionally, each individual cellular company maintains different information for different periods of time. For purposes of discovery, this may put litigants in a position where they seek information that is simply no longer available.

For instance, Verizon Wireless typically

stores call and text message detail records for only one-year, whereas Sprint typically stores this information for 18-24 months; T-Mobile stores this information for two years for a pre-paid user and five-years for a post-paid user; and AT&T "varies" on its retention. These "detail records" include only the number sent to and the date and time of the call or message. For text message content, Verizon Wireless typically stores this information for three to five days, whereas T-Mobile and AT&T do not retain message content.

Many cellular phone companies' subpoena divisions will attempt to notify the user its cellular phone data is being subpoenaed. The information will then be produced unless the court enters an order stopping the production. Whether looking to subpoena phone records or faced with a subpoena of your own records, you should consult with counsel to obtain or protect the information sought.



third party vendor can be retained to identify and disclose only those e-mails relevant to the dispute and to remove any privileged communications, such as e-mails to or from one's attorney or spouse.

But suppose your opposing party uses only web-based e-mail such as Yahoo or Gmail. You can ask that the opposing party produce all the relevant e-mails, but how do you know the party did not hold something back? Can you serve a subpoena on Yahoo or Gmail to obtain the e-mail communications?

The answer is, "Probably not." The reason is that web-based e-mail providers can invoke the Stored Communications Act ("SCA"), 18 U.S.C. § 2702, *et seq.* The SCA generally prohibits providers of electronic communication services from divulging "the contents of a communication" maintained by the provider. Although there are some exceptions to the rule — such as a subpoena issued by a law enforcement agency — every court that has addressed the issue has held that web-based e-mail providers cannot disclose electronic communications in response to civil subpoenas. This prohibition extends not only to e-mails, but also to text messages maintained by mobile phone carriers such as Verizon and AT&T Wireless. Some courts have also found that the

SCA prohibits the disclosure of private Facebook posts, i.e., posts visible only to your Facebook "friends," but does not prohibit the disclosure of Facebook posts that are viewable by all members of the public.

Note that the SCA prohibits only the disclosure of "the contents of a communication." It does not prohibit the disclosure of other information such as the identity of a particular account holder, IP address information, the date, time, and originating phone number of a text message, and other non-content information. This non-content information can be particularly useful in cases involving "hacking" or other unauthorized access to an electronic communication medium.

Finally, the SCA should not be viewed as a license to delete e-mails or other electronic communications that may be relevant to a brewing dispute. Litigants and potential litigants are obligated to preserve such information even in the absence of a formal request. This includes ensuring that relevant data is not overwritten in the normal course of business. Before disposing of e-mails or other electronic communications that may be relevant to a current or future dispute, you should always consult with counsel first.