# Obtaining Identities of Anonymous Online Defamers Just Got Harder

## By Debra L. Innocenti

The Texas Supreme Court limited a powerful tool in the libel litigator's toolbox this summer. In a 5-4 decision, the Court held that a Texas court cannot order a pre-lawsuit deposition to identify an anonymous online defamer if the individual does not have sufficient contacts with Texas for personal jurisdiction. *In re Doe a/k/a Trooper*, No. 13-0073, 2014 Tex. LEXIS 762 (Tex. August 29, 2014). The decision will likely compel victims of anonymous defamation and online bulling to rely on cyber investigation prior to resorting to litigation.

### The Decision

The Reynolds & Reynolds Co. and its CEO, Brockman, sought to depose Google, Inc. under Rule 202 of the Texas Rules of Civil Procedure to obtain the identity of a Google blogger using the nom de plume "Trooper." Trooper's blog posts allegedly discussed inside information at Reynolds and referred to Brockman as a "crook," comparing him to Bernie Madoff, Satan, and Bobo the Clown.

Reynolds gave Trooper notice by emailing a copy of the petition to his email address. Google, Inc. did not oppose the petition, but Trooper, appearing through counsel as "John Doe," did, asserting that the district court, by ordering discovery against Google, Inc., was adjudicating whether he had the right under the First Amendment to maintain his anonymity. Trooper filed a special appearance, asserting that his only contact with Texas was the availability of his blog online in Texas, which was insufficient contact for the exercise of personal jurisdiction. Accordingly, he argued, the Texas court was not a "proper court" under Rule 202 or, alternatively, that Rule 202 violated his procedural due process.

The Court agreed that the district court was not a "proper court" under the Rule. A "proper court," it held, must have personal jurisdiction over the potential defendant. It is plaintiff's burden to plead allegations showing the necessary jurisdiction. The Court "recognize[d] that this burden may be heavier in a case like this, in which the potential defendant's identity is unknown and may even be impossible to ascertain," but cautioned that "Rule 202 does not guarantee access to information for every petitioner who claims to need it."

The dissent warned that the decision will, at best, increase the costs of litigation and, at worst, deprive defamation victims from reparation, as anonymous online statements "are impossible to track without the help of the Internet service provider."

## What Happens Now?

As the decision curtails use of Rule 202, victims of defamers will likely need to rely on an initial cyber investigation to determine the location of their defamers before commencing a lawsuit.

A cottage industry has already cropped up around cyber investigation. It has been advertised as a more cost-effective way of identifying and neutralizing anonymous online bullies as opposed to litigation. A skilled cyber investigator can gather information available from the offending website, social media, or blog that can help pinpoint the defamer's geo-location. Doing so requires specialized detective work, including examining the content and timing of the defamatory material for clues as to the origin.

There is no easy roadmap for obtaining this information. Often it involves looking for a mistake or oversight by the anonymous defamer that reveals his or her identity. However, once the mistake becomes known in the online community, it is often not made again. For instance, a few years ago bloggers who used their Google's Analytics or Adsense accounts across multiple sites they owned, including their anonymous gripe sites, found themselves exposed. By using online reverse lookups of the account ID embedded in the source code, a cyber sleuth could determine whether blogs were using a common account. If they were, and one of those blogs had a public byline, odds were good that it was the same blogger. Very few (if any) anonymous bloggers make the Google Analytics mistake now, but new third-party plug-ins are developed every day, becoming popular and posing potential pitfalls.

A skilled sleuth can also employ "troll traps" to bring a defamer to an online location that is able to capture his or her IP address. This trick works if the cyberbully is especially aggressive and may be baited by an opportunity to comment on a blog or website feed. If the website or blog is enabled with tracking software, the cyberbully's IP address can be captured along with any comment. Once an IP address is obtained, online tools can drill down to the user's fairly exact location. A skilled cyberbully, however, may take precautions to mask his or her IP address.

The game changes every day. Software (such as the open source software Tor) is developed and upgraded to help mask a user's identity from network surveillance and traffic analysis. Correspondingly, techniques are developed and upgraded to attempt to exploit a weakness in the software.

Cyber investigation also presents ethics issues. Recent headlines have provided cautionary tales about lawyers – or intermediaries, such as investigators or legal assistants —accused of

unlawful “pretexting.” “Pretexting” occurs when an attorney engages in fraud or deceit to obtain evidence or information. Accordingly, careful consideration will need to be involved if some form of “pretexting” is used to bait a cyberbully to take a revealing action.

While the Trooper decision doesn’t make obtaining information “impossible,” as worried by the dissent, it will require libel litigators to be more technologically savvy in obtaining the evidence they need.

## About the Author

Debra L. Innocenti is a partner at Strasburger & Price LLP in the special litigation practice group. She resolves disputes and litigation related to financial services, the internet, and intellectual property. In connection with her Internet law practice, she assists software and web developers with terms of use agreements, privacy policies, license agreements, linking agreements, and general intellectual property issues. She is a member of Geekdom, and she was an instructor in the English-Communications department at St. Mary's University from 1997-2001.