How to Deal with Potential Defamation on Twitter

January 2015
The Online Reputation & Brand Protection Coalition’s mission is to help businesses protect their online reputations and brands online. The Coalition aims to fulfill its mission by educating businesses on how to protect and defend their reputations and brands online and advocating for increased protections and more effective remediation options for businesses.

Specifically, with respect to education, many businesses today are struggling because they do not understand how to best protect and defend themselves against online reputation and brand attacks, and there is presently a lack of quality educational materials and resources for businesses to turn to help understand and address these problems. To address the absence of these resources, the Coalition is committed to providing resources to businesses with the most up-to-date information designed to explain, prevent, and help businesses ultimately eradicate the problem of online reputation and brand attacks.

The Coalition provides its members with whitepapers created by the experts who regularly handle online reputation and brand attacks around the world addressing common reputation and brand problems which businesses are facing today.
I. Introduction

While Twitter is generally used in a positive manner, it is also a hotbed for trolling.

Although it took some time for the masses to adopt Twitter since the first public tweet was sent on March 21, 2006, Twitter has truly changed the way many people gather news and information and interact with others. While Twitter is generally used in a positive manner, it is also a hotbed for trolling. And beyond trying to provoke others, some bad actors go as far as posting defamatory content on Twitter, perhaps even creating Twitter accounts solely to disparage a business or person on Twitter.com or using the Twitter app. Depending on the particular user’s Twitter following and the specific content of his or her tweet, defamatory tweets can spread quickly, although it is only necessary that one third party views defamation for it to be actionable.¹

People who have private accounts or delete potentially defamatory tweets cannot assume these tweets will not go (or have gone) unseen. Moreover, bad actors who send out false and disparaging tweets cannot assume they are immune from the consequences of defaming others on Twitter, even if they have shielded their identities and do not publicly display any identifying information. In fact, when a person or company believes they have been defamed by an unknown user, that party may be able to identify the person behind a particular Twitter handle (i.e. @username) and tweet (or series of tweets). Specifically, they can work with an attorney to issue a subpoena to Twitter to obtain personally identifying information for the user, such as Internet Protocol (IP) addresses and an email address.

This whitepaper will discuss the process of handling defamation on Twitter, including how to use the subpoena process to identify Twitter users publishing defamatory content.

¹ Of course, the more people that see it, the more harmful; if only one person were to view a defamatory tweet, it would not be worth pursuing a defamation action.
How to Deal with Potential Defamation on Twitter

II. Monitoring for and Responding to Twitter Attacks

As discussed in the “Comprehensive Guide to Protecting & Defending Against Online Reputation Attacks,” businesses must monitor their internet and social media mentions in order to identify potential threats as soon as possible. Often times, tweets mentioning another’s Twitter account will automatically generate emails sent to the mentioned party, so a company’s social media manager or whomever runs its Twitter account, might see some of these tweets. They may also consider checking the account’s “Notifications” page directly on Twitter.com or on the Twitter app to similarly view tweets mentioning the business’s @username:

Of course, neither of these approaches accounts for tweets that feature comments about a company that do not include its actual Twitter handle (e.g. “Wow, totally got ripped off by CompanyABC123. What a scam! #screwedmeover”). Therefore, a better practice is to utilize a social media management tool such as Hootsuite or TweetDeck, which aggregates and organizes different “streams” of tweets for Twitter users, such as replies or mentions (tweets including the Twitter handle), and tweets simply containing certain key words (e.g. company or brand name). This will better facilitate the identification of potential attacks such as defamation. Companies with small followings (perhaps a hundred or fewer followers) do not need to monitor tweets as much as a company with, say, thousands or millions of followers. For example, Starbucks Coffee (6.99 million followers) and McDonald’s (2.67 million followers) need to monitor more regularly than, say, a ma and pa shop. But every business must keep tabs on what is being said about it online.

When a business identifies a potentially harmful tweet, the suitable party or parties – noting that larger companies may have various parties to turn to, including outside consultants – should gather as much information as quickly as possible and determine if it warrants a reply or some other action. In many instances, a potentially defamatory tweet may be nothing to worry about. For example, if the tweeter has very few or actual no followers. Of course, taking no action can also provoke bad actors to repeat their attacks in order to get attention.

Nevertheless, it is still important for businesses to be prepared to appropriately respond when the situation does warrant a response, especially in terms of being able to persuade the attacker to remove the defamatory content. Convincing a party to remove defamatory tweets may include preparing to take legal action and, accordingly, alerting the user that it is prepared to take legal action. Without an email address or physical address, a business will be unable to send a traditional cease and desist letter. However, it does have the ability to privately message a

---

2 Essentially, in the case of a business, anytime other Twitter users send tweets that include that particular business’s Twitter handle/@username, whether at the beginning, in the middle, or at the end of those tweets (for example, “@CompanyABC123 ripped me off. What a scam!” “Just got ripped off by @CompanyABC123. What a scam!”).

3 See the “Comprehensive Guide to Protecting & Defending Against Online Reputation Attacks” whitepaper for more on key questions to ask in the monitoring/identifying stages.
How to Deal with Potential Defamation on Twitter

...address the defamatory tweet by persuading the attacker to delete the tweet and/or pursuing legal action...

user (although each “direct message” is also limited to 140 characters).

In short, a party defamed on Twitter should either: 1) ignore the attacker/attack(s) altogether or 2) address the defamatory tweet by persuading the attacker to delete the tweet and/or pursuing legal action and (assuming his or her identity is unknown) issuing a subpoena to Twitter.
III. Identifying Anonymous Twitter Users Via Subpoenas

A. The Basics of a Subpoena to Twitter

When a defamatory tweet, or perhaps a series of tweets, poses a serious threat, it is often recommended that a business utilize an attorney to issue a subpoena to the San Francisco-based Twitter, Inc., seeking personally identifying information about the user. This process involves first filing a “John Doe” lawsuit against the user, preferably in the jurisdiction in which its principal place of business is located. Where a lawsuit is filed is important to the subpoena process, as each state handles subpoenas differently. Once a valid lawsuit for defamation and/or business torts has been filed and the business has a case number, its attorney can proceed with preparing and issuing the subpoena to Twitter in California.

If a case is pending outside California, the business’s legal counsel must be aware of what the forum state requires for serving discovery in another state. Many states require the local subpoena to be issued by the clerk of the court in which the action is pending, as opposed to being issued by the attorney himself or herself. Some states, such as Texas, may require requesting a commission or letter rogatory from the court in order to conduct out-of-state discovery. This essentially means asking the local judge to give an order to another state’s court requesting the issuance of a subpoena in the pending case.

Subpoenaing Twitter is easiest when the case is pending in California, as it will not require a supplemental subpoena from another state. Either way, California does permit a party to a case pending in a foreign jurisdiction to retain a California-licensed attorney to help execute and issue the appropriate California subpoena form (as opposed to opening an entirely new matter in the state, as some other states may require, such as Illinois). The specific California form to use will vary by case. The most common forms used when issuing subpoenas to Twitter are SUB-010 (Deposition Subpoena for Production of Business Records) and SUB-035 (Subpoena for Production of Business Records in Action Pending Outside California), both of which can be easily found using a search engine (as well as the MC-025 form for attachments).

4 Pursuant to Section 230 of the Communications Decency Act, Twitter itself cannot be held liable for false or defamatory statements made by its users.
5 Twitter’s registered agent is: CT Corporation System, 818 West Seventh Street, 2nd Floor, Los Angeles, CA 90017.
6 Pursuant to Texas Rule of Civil Procedure 205, however, Texas does alternatively permit litigants to provide 10 days’ notice to the non-party to which the subpoena is being issued, in lieu of obtaining a letter rogatory (this is often more efficient than waiting for a judge to approve a letter rogatory).
8 Definitions/instructions and the actual requests for items to be produced can go here. If MC-025 does not provide enough space, the issuing party may type “See attachment” and include this information on a separate typed page.
How to Deal with Potential Defamation on Twitter

An IP address, as discussed below, is the most valuable piece of information.

B. Drafting a Subpoena that Twitter Will Not Find Objectionable

Signing up for a Twitter account entails providing a full name, an email address, creating a password, and choosing a username. Thus, when it comes requesting information from Twitter, the subpoena served on Twitter should generally be limited to asking for the user’s name, his or her email address, perhaps the date and time of the account creation, and certainly internet protocol addresses and/or IP log data. An IP address, as discussed below, is the most valuable piece of information. Of course, requesting parties must keep the following in mind:

» Twitter does not verify (or require) real names;

» Twitter does not verify email addresses (though, presumably, any email address provided is legitimate, even if it is not one the Twitter user actually uses beyond setting up a Twitter profile);

» Certain information such as IP logs may only be stored by Twitter “for a very brief period of time”; and

» Twitter retains user data for just 30 days after an account has been deactivated.10

In other words, subpoenas to Twitter should be narrowly tailored, as Twitter’s counsel will object if subpoena requests are overbroad (they must be reasonably

9 Source: https://support.twitter.com/articles/41949-guidelines-for-law-enforcement#
10 Source: https://support.twitter.com/articles/15358#
How to Deal with Potential Defamation on Twitter

11 Technically, all entities require this, but many seem to give the requesting party the benefit of the doubt (or allow them to submit an affidavit from the plaintiff showing its claims can survive a motion for summary judgment).

12 We recommend obtaining an order from the court that finds compliance with the law relating to anonymous posters, such as convincing a judge to issue an order permitting the plaintiff to conduct discovery.

13 See Dendrite Int’l, Inc. v. Doe, 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001) and John Doe No. 1 v. Cahill, 884 A.2d 451 (Del. 2005), each establishing standards that must be met before a court will permit an anonymous speaker’s identity to be unmasked. For instance, Dendrite requires a plaintiff to: 1) attempt to notify the speaker his/her identity is being sought; 2) identify, verbatim, the allegedly actionable speech; 3) allege all elements of the claim; 4) present sufficient evidence supporting each element; and 5) prove to the court the right to the speaker’s identity outweighs the speaker’s right of anonymous free speech.


15 Using a website such as: http://whatsmyipaddress.com/ip-lookup (see screenshot above).

16 Of course, this is a bit oversimplified, as there may be other hoops to jump through. For example, if the ISP is a cable provider, such as Time Warner Cable or Comcast, it is necessary to get a court order authorizing the ISP to disclose subscriber information, pursuant to a federal privacy law. The requesting party can also attempt to issue a subpoena to the email provider, for instance Google, Yahoo, or Microsoft, if the subpoena also produces an email address.

The short of it is that Twitter will not release any information without the court in which the action is pending first determining that the plaintiff has demonstrated that its claims meet the standards for unmasking anonymous posters. More specifically, Twitter seeks documentation that demonstrates the court considered and imposed the First Amendment safeguards required before the litigant is permitted to unmask the speaker’s identity.

Courts have generally adopted the tests in Dendrite and Cahill, and the California Court of Appeal has adopted a test that requires: (1) an attempt to notify the affected speaker; and (2) a prima facie showing of the cause of action for defamation or libel before a plaintiff can discover the identity of an anonymous online speaker. Regarding the former, upon receipt of a valid subpoena, Twitter will attempt to provide notice of the subpoena to the affected user(s) informing them of their right to file an objection with the court or affirmatively authorizing disclosure. If there is no objection, Twitter will produce the requested information.

If Twitter does produce an IP Address, the requesting party can generally determine the internet service provider (ISP) and issue a subpoena to that ISP for documents/information related to the subscriber who posted on Twitter. Once the unknown or anonymous Yelp reviewer is identified through this process, the business can name them as a defendant in its lawsuit and continue to pursue its claims.

While we generally recommend issuing a subpoena to Twitter, a business can also attempt to identify an unknown Twitter user using a cyber investigator or having a forensic exam conducted, as discussed in “How to Identify Anonymous Persons Attacking Your Business Online.”
IV. Conclusion

As mentioned, in addition to narrowly tailoring requests, the requesting parties are strongly advised to obtain a court order to present to Twitter’s counsel with the subpoena.

Twitter may limit tweets to 140 characters or less, but that character limit is not stopping many people from posting defamatory content through their accounts. While Twitter is more strict than many others in terms of how it goes about accepting subpoenas and producing requested information, by following the above recommendations, a business has a favorable chance of unmasking an unknown Twitter user. As mentioned, in addition to narrowly tailoring requests, the requesting parties are strongly advised to obtain a court order to present to Twitter’s counsel with the subpoena.