Subpoena Guide for Identifying Anonymous Internet Posters:

How to Navigate the Subpoena Process in Response to Online Attacks

VORYS

Higher standards make better lawyers.®

This Subpoena Guide is intended to help attorneys and businesses navigate the complex process of issuing subpoenas to third-party websites and internet service providers to identify anonymous online attackers. It provides an overview of the steps to be taken and items to be considered in various circumstances when subpoenaing non-party entities as part of your response to online attacks.

State Subpoenas

Many internet-related legal claims against anonymous defendants are brought under state law, meaning they require the issuance of subpoenas at the state level. Therefore, it is important for practitioners to be aware of the subpoena rules in their own states, as well as the "foreign" rules in the states where they intend to issue their subpoenas.

As discussed below, if your client has been harmed by an anonymous person who created a false posting online or performed some other bad act on the internet, the first entity you will want to subpoena is the third-party website on which the anonymous person posted. Therefore, it is necessary to first identify where the entity or website you intend to subpoena is located and has registered agents.

Many websites or internet companies are headquartered in one state but incorporated in another (usually Delaware). Others are registered and headquartered in a single state. But sometimes a company has registered agents in several states. For example, Facebook is incorporated in Delaware, headquartered in California, and has several offices throughout the United States (and in other countries).

Ideally, the website you will be dealing with is registered to do business in the state in which your lawsuit is pending. In this situation, simply issue a subpoena duces tecum to the website's registered agent, pursuant to the state statute/local rules of your forum. If the website is not registered in the forum in which your lawsuit is pending, you will need to issue a foreign subpoena. Before you do so, be sure to thoroughly review the rules in both your home state and the state in which you wish to issue the subpoena.

Knowing Your Own State's Rules

Before you issue a subpoena in a state case, first consider the forum state's rules, as well as accepted local practices.

If you need to issue foreign discovery, determine if you are required to request a commission (called a letter rogatory in some jurisdictions) from your own court. Requesting a commission essentially means asking a local judge to give an order to another state's court requesting the issuance of a subpoena in your pending case.

Few states require a commission on their own terms, but you may need a commission anyway, as discussed below. Furthermore, even when the rules do not specifically outline such a procedure, local practice may require requesting a commission.

Before you unilaterally engage in foreign discovery, also consider possible requirements of providing notice to other parties. As many internet matters begin with John Doe defendants, oftentimes notifying the other parties of the discovery you are prepared to conduct is impossible. However, in matters where at least one other party is named in the litigation, be mindful of the governing rules related to third party notice.

Know the Relevant Foreign State's Rules

If you need to issue a subpoena in a state other than the one in which the case is pending, once you are armed with the knowledge of what the forum state requires for serving discovery, check the rules of the foreign state.

Some states, such as California, will allow a subpoena to be served on a party in their jurisdiction simply by having an attorney licensed to practice in the particular state execute the subpoena. *See* Cal Code Civ Proc § 2029.350. California has a form specifically for production of documents in actions pending outside the state.

Others require a few additional steps in order to have a subpoena executed by the clerk of courts in that jurisdiction. For example, Arizona requires presenting a foreign subpoena (which must include the phrase "For the Issuance of an Arizona Subpoena Under Ariz. R. Civ. P. 45.1") to the clerk of the relevant Arizona county, along with an Arizona subpoena. *See* Ariz. R. Civ. P. 45.1.

Illinois, among others, requires a party to open a miscellaneous matter in that state. Under Ill. Sup. Ct., R 204(b), an Illinois attorney may then petition the relevant Illinois circuit to issue a subpoena duces tecum and compel another party to produce the documents requested in that subpoena. This is costly and time-consuming, and it requires steps such as hiring an attorney and paying the associated filing fee.

Finally, some states require the aforementioned commission or letter rogatory in order to execute a subpoena for the discovery. Thus, you may need a commission from the forum state, even if that state otherwise does not require you to obtain one.

New Jersey, for example, requires obtaining a commission from the forum state. Then, similar to Illinois, under *R.* 4:11-4 a New Jersey-licensed attorney may petition the Superior Court of New Jersey for an order authorizing the issuance of the subpoena. Specifically, the attorney would need to file an *ex-parte* petition in the relevant county, a proposed form of order, and the proposed subpoena. Upon receipt of the signed order and subpoena, the attorney can then issue the subpoena.

*** *Practice Tip*: Check if the state has enacted the Uniform Interstate Depositions and Discovery Act (UIDDA), which provides litigants with simple standardized procedures for subpoenaing out-of-state parties and the production of discoverable materials located outside the forum state. Every state that has incorporated the Act (more than half) will have its own take on the UIDDA. Some states only allow a subpoena to be issued under the requirements of the UIDDA if the foreign state from which someone is requesting discovery also has enacted the UIDDA. North Carolina law, for example, reads that, "In applying and construing [the UIDDA], consideration shall be given to the need to promote uniformity of the law with respect to its subject matter among states that have enacted the Uniform Interstate Depositions and Discovery Act." N.C. Gen. Stat. § 1F-7.

Federal Subpoenas

Federal subpoenas are easy to execute. Pursuant to Fed. R. Civ. P. 45(a)(3), any attorney authorized to practice in the issuing court may execute a federal subpoena, using the appropriate federal form. This includes an attorney admitted *pro hac vice.*

As experienced federal practitioners are aware, no discovery is to be completed in a federal case until the Rule 26(f) conference has taken place. Thus, federal subpoenas are only useful if you have had a conference of the parties, in accordance with this rule.

If you have discovery that you need to conduct in a timely fashion and/or the defendant is currently a John Doe (in which case there is no identifiable opposing party with whom to have the 26(f) conference), you will have to file a Motion requesting Leave from the Court to conduct this discovery prior to the 26(f) conference.

Subpoenaing Websites: *Meeting the* Dendrite *Standard*

The Supreme Court of the United States has stated that anonymous free speech is protected under the First Amendment. *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 342 (1995). Thus, before you issue a subpoena for the identity of an anonymous poster, make sure you can survive a Motion to Quash the subpoena, should the anonymous person object on First Amendment grounds.

Check the caselaw in your jurisdiction to see if this issue has been addressed by courts in your jurisdiction *before* issuing the subpoena. This will ensure that prior to spending time and resources pursuing a claim against an anonymous defendant, you have a viable claim and will not end up using client resources to pursue a matter in which you cannot even get to the step in which you identify the defendant.

Most courts follow the standard set forth in the New Jersey appellate court decision of *Dendrite Intern., Inc. v. Doe No. 3*, 775 A.2d 756 (2001). Under the *Dendrite* standard, courts typically allow plaintiffs to conduct discovery to identify anonymous defendants if a plaintiff can show: (1) An 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, on balance and in the particulars of the case, the right to identify the speaker outweighs the First Amendment right of anonymous speech.

Practically, this means you should be aware of providing notice to the anonymous speaker of your subpoena; you should be able to identify the specific statements/words that are the basis of your claim (not just "Report #123"); and have a complaint that outlines every element of the cause of action, and have some evidence – whether in the form or affidavit or otherwise – that shows you can meet the elements of your claim. For practical purposes, you should be able to defeat a motion for summary judgment at a very initial stage, by coming forward with evidence supporting your claims.

If you are unable to find caselaw in your jurisdiction that is on point, a safe bet is to ensure you meet the *Dendrite* standard.

What to Request in the Subpoena

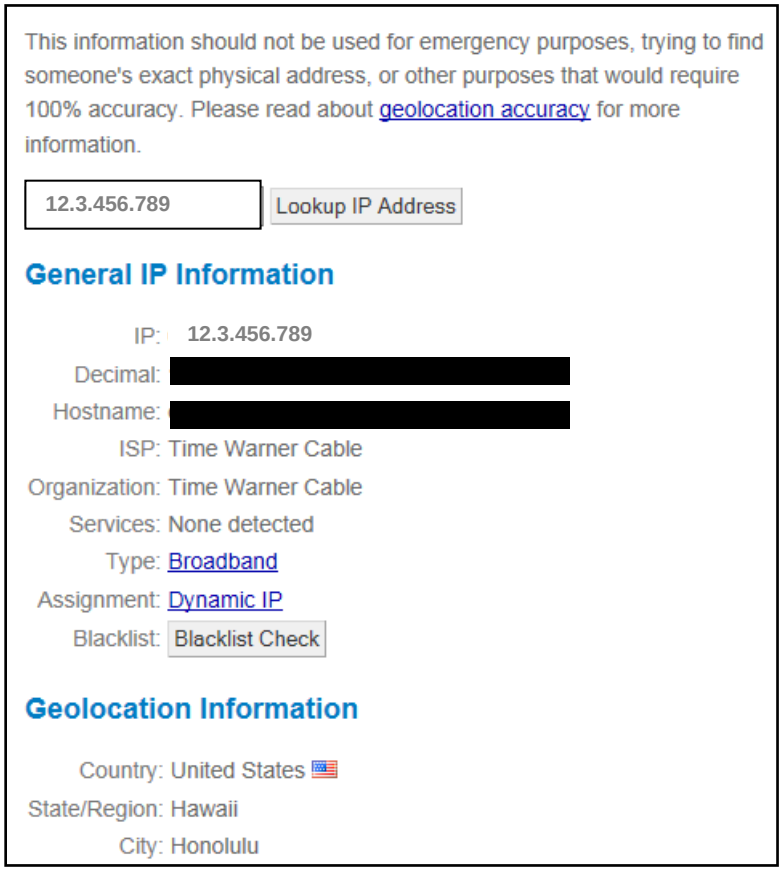
When requesting information from a website, you will want to ask for any personally identifying information the website may have regarding the poster. This would include, but is not limited to, the poster's first and last name, address, phone number, email address, and Internet Protocol Address (IP Address) and IP logs.

Keep in mind, each third-party website requires different information from its users upon registration. For example, some do not require an active email address and many do not require a first and last name. Further, most websites do not verify any of the personal information a person supplies when he or she registers an account. Thus, while it is rare that you will receive valid information regarding an anonymous user's actual name or address, but it is worth asking. In some instances, the potential defendant may not have realized that this information is

discoverable and, accordingly, may have provided identifying information upon account registration.

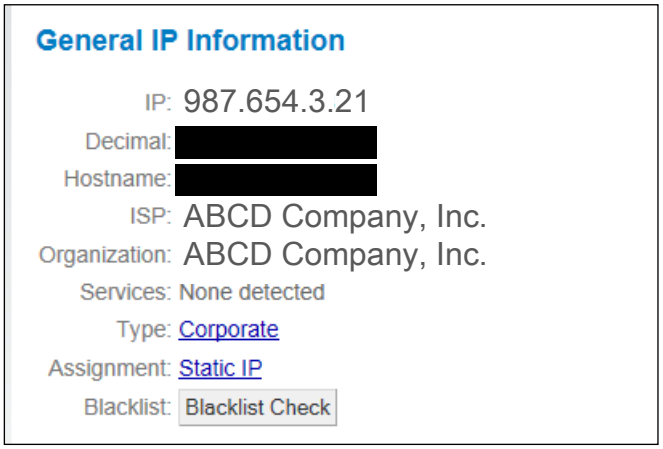
Also note that when a subpoena is issued to a third-party website, the website may object to an appearance at the place of production. In this situation, the website will likely just produce the requested information, accompanied by an authenticating affidavit.

Because individuals very rarely use their real name and/or email address to register and/or post on a website, oftentimes, the most valuable piece of information a website can provide is the IP Address. The IP Address will lead you to where the person posted the content from – hopefully, for you, their residence. Once you obtain an IP Address from the subpoena to the third-party, you must determine where it is registered. This can be completed by simply searching for the IP Address on one of the many public IP Address locator forums online. Through this search, you can also find the Internet Service Provider (ISP) that owns that particular IP Address. A search result from http://whatismyipaddress.com/ip-lookup looks like this:



This screenshot of the search of hypothetical IP Address "12.3.456.789" on www.whatismyipaddress.com shows the name of the ISP and location – in this case, Time Warner Cable (TWC) and Honolulu, HI – among other information provided.

Many companies have their own IP Addresses, so in some circumstances – such as if a person defamed another individual while using his or her work computer – you might need to contact the particular company's counsel or work with its IT department to try to trace the online activity to a specific computer.



Subpoenaing Internet Service Providers

Once an IP Address is acquired and the specific ISP is determined, the next step is to subpoena that ISP for information relating to the customer that was using that IP Address at the date and time in question. It is important to remember that, for most residential IP Addresses (like in the first example/screenshot above), the IP Address is "dynamic" – that is, the IP Address assigned to a certain customer changes sporadically, so it is critical to have the date and time of the post that is at issue; without it, the ISP cannot give you the information you are seeking.[1]

Alternatively, if an IP Address is "static," this usually indicates a business is using the IP Address. In some instances, depending on the particular business, it may not be possible to identify the poster – for instance, if the business provides free Wi-Fi from which the poster published his or her harmful content.

Once the ISP is identified, look up the registered agent in the appropriate state for the ISP and serve a subpoena. Comcast is in 39 states plus Washington, D.C., and TWC has customers in 29 states, for example, so you would not automatically serve the ISP where it is incorporated or headquartered. Again, ideally the ISP will be registered in the state in which your lawsuit is pending, which is often – though not always – the case.

Some ISPs, such as TWC and Comcast[2], are cable providers, meaning they are subject to the Cable Privacy Act, 47 U.S.C. § 551. Such entities are prohibited from releasing any personally identifying customer information, absent a court order. Specifically, pursuant to 47 U.S.C. § 551(c)(2)(B), a "cable operator may disclose such information if the disclosure is … made

[1] Because residential IP Addresses are dynamic, one must be aware of the time limitations that ISPs have on providing this information in response to a subpoena. Most cable companies only keep this information for six months. Other entities keep it for nine months to a year, but preservation policies are constantly changing. Thus, time is of the essence when you are subpoenaing information related to an anonymous poster.

[2] In February 2014, Comcast Corp. agreed to buy Time Warner Cable for $45.2 billion. The transaction, expected to be finalized in late 2014, was not yet completed at the time of the Subpoena Guide's publication.

pursuant to a court order authorizing such disclosure, if the subscriber is notified of such order by the person to whom the order is directed."

Thus, when attempting to subpoena customer information from a cable provider ISP, it is necessary to file a Motion with the Court requesting an Order allowing the cable company to release the information. This is an additional step, and one that more or less comes down to luck: did the potential attacker personally subscribe to or post from an IP Address belonging to someone who subscribed to a cable provider or a phone or internet provider?

About the Author:

Whitney Gibson is a partner at Vorys, Sater, Seymour and Pease LLP and leader of the firm's internet defamation group. The group has worked on hundreds of internet related cases from across the country and develops unique solutions for companies being damaged or attacked online. Mr. Gibson has experience in all aspects of internet of law, including defamation, false reviews, traffic diversion, product diversion, trademark infringement, SEO manipulation, copyright infringement and public disclosure of private facts. He can be reached at 855.542.9192 or at wcgibson@vorys.com.

This guide is for general information purposes and should not be regarded as legal advice. Please contact the authors if you want more information or have questions about how these concepts apply to your situation.