The Computer & Internet Lawyer

Volume 35 ▲ Number 3 ▲ MARCH 2018

Ronald L. Johnston, Arnold & Porter, LLP, Editor-in-Chief

Doe Hunting: A How-To Guide for Uncovering John Doe Defendants in Anonymous Online Defamation Suits

By Savanna L. Shuntich and Kenneth A. Vogel

Envision a car dealership named Greater Maryland Auto World, owned by a stalwart member of the community named Charles Woolworth McHuggins VI. Mr. McHuggins is an active member of the Lion's Club, a major donor to the Chesapeake Bay Foundation, an announcer for his local high school football team, and the beloved grandfather of 12 apple-cheeked grandchildren. Assume that Mr. McHuggins has a smaller competitor called "Tom's Toyota" located one state over, in Delaware. Owner Tom Smith aspires to Mr. McHuggins's level of success. Mr. Smith wants to expand to Maryland, but he is afraid that he will not be able to break into the market due to the dominance of Greater Maryland Auto World.

Kenneth A. Vogel practices at Bar-Adon & Vogel, PLLC, a general business and litigation law firm in Washington, DC, with an emphasis on real estate and construction disputes. **Savanna L. Shuntich** practices employment law at Alderman, Devorsetz and Hora PLLC. This article originally appeared in the *Maryland Bar Journal* and is republished here by permission of the Maryland State Bar Association.

In a jealous rage at the continued success of Greater Maryland Auto World, Mr. Smith decides to go rogue and fund a defamation campaign against Greater Maryland Auto World and that charming pillar of the community, Charles Woolworth McHuggins VI. Mr. Smith covertly hires a web designer to create a Web site entitled *www.CharlesMcHugginsIsTheWorst.com,* which claims that Mr. McHuggins underpays his workers, passes off used cars as new, and spends his free time torturing puppies, all of which are untrue. In addition, Tom Smith established an email address under the name of *UnhappyCarBuyer@gmail.com*. Using the new email address, Mr. Smith posted negative online reviews on Yelp about Greater Maryland Auto World.

Mr. McHuggins is understandably aghast at the contents of *www.CharlesMcHugginsIsTheWorst.com*. He comes to you, his long-time attorney, seeking help. He wants to sue the person responsible for the Web site for defamation, and he wants the Web site taken down. In the Internet age, this scenario is becoming common. Successfully prosecuting one of these cases presents a unique set of

Wolters Kluwer

challenges because of the complex E-discovery required to unmask online John Does. Business lawyers may very well have clients who voice concerns about online anonymous defamatory Yelp and Amazon reviews, Twitter tweets and Facebook postings, or a standalone Web site (to give just a few examples).

It is impossible to recover a money judgment against a John Doe. This article explores how to find John Doe, an unknown speaker, who is anonymously voicing opinions on the Internet. Once John Doe is identified, one can pursue an ordinary defamation claim. First, the article discusses threshold issues attorneys should consider before filing a John Doe lawsuit. Next, it describes the first phase of discovery, which involves, if in federal court, getting a court-order authorizing early discovery and writing subpoenas that comply with the federal Stored Communications Act. Finally, it will detail the second phase of discovery when subpoenas are sent to Internet Service Providers (ISPs). The Plaintiff may need to contend with the John Doe's right to remain anonymous under the First Amendment.

Initial Considerations

Initial considerations for one of these cases include the state's statute of limitations on defamation, securing E-discovery vendors, and the federal Communications Decency Act.

Statutes of limitations run quickly in defamation cases. For example, in Maryland, the Statute of Limitations for defamation is only one year. Md. Code, Courts and Judicial Proceedings § 5-105. Other states have similar short statutes of limitations. This may not seem like a problem because the defamatory online content is always accessible and continues to cause the client harm every single day it remains online, but Federal courts in Maryland and in other jurisdictions have adopted the "single publication rule." In *Hickey v. St. Martin's Press, Inc.* the District Court explained "[u]nder the 'single publication rule,' only one action for damages can be maintained as to any single publication. Under the 'multiple publication rule,' every sale or delivery of the defamatory article is viewed as a distinct publication which causes injury to the defamed person and creates a separate basis for a cause of action."[1] In other words, the minute that the defamatory comment, Web site, etc. goes live the Statute of Limitations begins to run even if the injured party does not discover the defamation for months. In Mr. McHuggins's case, the statute began to run when the Web site was made accessible to the public, not when Mr. McHuggins first learned of the Web site. The Maryland Court of Appeals has yet to address the issue, but to quote the federal court in *Hickey* "[f]ollowing its review of the applicable authorities, this court has concluded that the Court of Appeals of Maryland would adopt the single publication rule if the question were presented to it in this case."

Another thing to be mindful of is the amount of technological expertise these cases entail. Any attorney hoping to undertake an anonymous defamation case must have a good E-discovery sleuth. The average attorney knows very little about IP address logs, MAC addresses, hosting services, proxy agents, and any of the plethora of other technology these cases entail. Even comments on legitimate Web sites such as Yelp can be made anonymously through fake registration information. This may require several rounds of subpoenas *duces tecum* to uncover John Doe. The right E-discovery vendor can help craft subpoenas and follow the trail of the John Does through the Web.

The average attorney knows very little about IP address logs, MAC addresses, hosting services, proxy agents, and any of the plethora of other technology these cases entail.

On a final note, the Federal Communications Decency Act (CDA) limits liability in online defamation cases by protecting third party publishers of defamatory content. This law was passed in the late 1990s and has been controversial. It states in pertinent part "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[2] Practically, this means that you can only sue the John Doe(s), not the platform where the defamatory content appears. In the hypothetical that began this article, there was a defamatory Web site. This means that a company like GoDaddy would have registered the domain name for the site. A separate company might provide the hosting service for the Web site. The domain registrar and the hosting company are immune from liability under the CDA. Mr. McHuggins may only sue John Doe. There are various CDA reform movements afoot, but for now only the current language of the CDA is relevant. Plaintiffs generally name multiple John Does in case more than one individual participated in the defamation. Courts are accustomed to seeing cases with captions such as "McHuggins v. John Does 1-10."

Round One of Subpoenas

Most litigators deal with the discovery process on a daily basis. Litigating anonymous online defamation disputes feels backwards because typically attorneys

issue discovery only after there is an identified defendant. Federal Rules of Civil Procedure 26(f) requires that attorneys hold a discovery conference with opposing counsel prior to seeking discovery from any source. Without an identifiable defendant with whom to conference, the Court must authorize early discovery under Rule 26(d) which states "[a] party may not seek discovery from any source before the parties have conferred as required by Rule 26(f), except … when authorized by these rules, by stipulation, or by court order." If the case is in federal court, the plaintiff needs to file a motion requesting early discovery before anything else. There is no comparable rule in Maryland state courts.

Either with or without a court order (depending on the jurisdiction) the next step is to begin issuing *subpoenas duces tecum* to companies and individuals who may have identifying information about the John Does. Principally this means subpoenaing the technology platforms where the defamatory content appears. For example, in our hypothetical, Mr. Smith wrote a defamatory Yelp review about Mr. McHuggins. In that case he would subpoena Yelp for any and all documents pertaining to the anonymous speaker's Yelp account. For the anonymous Web site, subpoenas would be issued to the domain name purveyor (companies such as GoDaddy and Namecheap) and the domain hosting service (companies such as DreamHost and HostGator).

In seeking discovery against technology companies, defamed plaintiffs are severely limited by the Stored Communications Act (SCA).[3] The SCA places restrictions on companies in the business of offering an "electronic communication service" that Congress defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[4] In response to a subpoena or other request, "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service … ."[5] This limits the discoverable information from companies to non-content, such as addresses, phone numbers, email addresses, account recovery information, and IP addresses. Colloquially, this is known as basic subscriber information or "BSI." It may be that the John Doe(s) used fake contact information, such as a registered address of 123 Main Street, Baltimore, MD 21218, or a false email address such as *TheRealCharlesMcHuggins@gmail.com* or a "burner" phone. If so, the most important information one can request is the user's IP address logs.

"[A]n IP (Internet Protocol) is an address assigned by your Internet Service Provider (ISP) and is used to give your computer or other device access to the Internet."[6] IP addresses are either static or dynamic. Most customers have a dynamic IP address. With a dynamic IP address, the ISP assigns a temporary IP address to its customer. It can later re-assign the IP address to another customer based on the ISP's need at any time without notifying the customer. Over time, a single customer will use many different IP addresses. This presents a problem for the IT investigator as the dynamic IP address used to post defamatory material may on one day belong to one customer, and on another day be re-assigned to some innocent person who is unrelated to the defamatory posting. Static IP addresses are more expensive and never change. "For companies with secured networks, a device with a static IP address helps the network administrator open their network to the specific address, which gives you access to the company intranet. Medium and large-sized accounts, primarily business accounts, often need static IP addresses. This feature is not for everyone."[7] In the case of IP addresses, the address is affiliated with the network, not an individual computer.[8]

ISPs keep records of whom they have assigned a particular dynamic IP address in the past. If the Web hunter can track the defamer to a static IP address or previous dynamic IP address you know from where the Web content was uploaded.

When IP address logs are provided, they may come from a number of sources of varying degrees of reliability. Maybe the perpetrator used the open wireless network at a local Starbucks to work on *www.CharlesMcHugginsIsTheWorst.com*? In that case, the IP address registered would be the IP address for a specific Starbucks. Any customer logging in at that same Starbucks would register the same IP address. These IP addresses help little in identifying John Doe. But if John Doe used a work computer at his office to create the Web site, his business might have a static IP address. This same IP address is recorded from every other employee at the company location, but it gets you closer to the culprit. Ideally you can get a static IP address linked to someone's small business or home network. This makes it fairly easy to determine the identity of John Doe. Locating dynamic IP addresses can still prove useful. ISPs keep records of whom they have assigned a particular dynamic IP address in the past. If the Web hunter can track the defamer to a static IP address or previous dynamic IP address at Tom's Toyota, you know from where the Web content was uploaded.

A final word of caution: Do not always expect to obtain the user's true IP address. If John Doe is tech-savvy he may be using a proxy service to cloak his true IP address. A proxy service reroutes a user's Internet connection and can make his location appear to be originating from anywhere on earth. *HideMyAss.com* provides such a service. With enough time and financial sacrifice, it is possible to trace an IP back to the point of origin but be prepared for the possibility of a never-ending rabbit hole. In addition, if the company providing the IP address spoofing is abroad, they will not comply with subpoenas issued by American courts.

IP Addresses, Anonymous Speech, and the First Amendment

The final step in the discovery process is to subpoena the ISPs that issued the IP addresses received in response to the first round of subpoenas. Content carriers such as Facebook will only provide basic subscriber information, but the requests might still yield the contact information for the John Doe. There is an added wrinkle at this stage because "[i]ncluded within the panoply of protections that the First Amendment provides is the right of an individual to speak anonymously."[9] Courts have determined that "this protection extends to anonymous speech on the Internet."[10] To win a motion to compel or fend off a motion to quash the subpoena you will need to show the court why the Plaintiff's need for the information should overcome John Doe's First Amendment rights. Courts are not in agreement as to how best to protect the First Amendment rights of anonymous online speakers.[11] There is not sufficient space in this article to discuss the wide array of tests courts have crafted to "appropriately balance a speaker's constitutional right to anonymous Internet speech with a plaintiff's right to seek judicial redress from defamatory remarks."[12] Among the best known are *Dendrite International, Inc. v. Doe*,[13] and *Doe v. Cahill*.[14]

The Maryland Court of Appeals explicitly adopted the *Dendrite* test in the 2009 opinion in *Independent Newspapers, Inc. v. Brodie* authored by Judge Lynne Battaglia.[15] In *Brodie*, the Plaintiff objected to several anonymous posts on a newspaper's online message board that called his Dunkin Donuts restaurant filthy and said the establishment was "wafting" trash into the nearby river.[16] The *Dendrite* standard, as articulated by the Maryland Court of Appeals, is as follows:

> Thus, when a trial court is confronted with a defamation action in which anonymous speakers or pseudonyms are involved, it should: (1) require the plaintiff to undertake efforts to notify the anonymous posters that they are the subject of a subpoena or application for an order of disclosure, including posting a message of notification of the identity discovery request on the message board; (2) withhold action to afford the anonymous posters a reasonable opportunity to file and serve opposition to the application; (3) require the plaintiff to identify and set forth the exact statements purportedly made by each anonymous poster, alleged to constitute actionable speech; (4) determine whether the complaint has set forth a *prima facie* defamation *per se* or *per quod* action against the anonymous posters; and (5), if all else is satisfied, balance the anonymous poster's First Amendment right of free speech against the strength of the *prima facie* case of defamation presented by the plaintiff and the necessity for disclosure of the anonymous defendant's identity, prior to ordering disclosure.

The US District Court for the District of Maryland has yet to adopt a particular standard. In *In re Subpoena of Daniel Drasin Advanced Career Technologies, Inc. v. John Does 1-10,* the Maryland Court indicated a preference for the *Dendrite* standard.[17] The McHuggins anonymous Web site criticized both McHuggins's business and personal character. In *In re Subpoena of Daniel Drasin,* Maryland's US District Court suggested that the *Dendrite* standard might not be appropriate for defamatory commercial speech because "courts typically protect anonymity in literary, religious or political speech, whereas commercial speech … enjoys a limited measure of protection, commensurate with its subordinate position in the scale of First Amendment values."[18] On the other hand, personal, religious, and political free speech enjoy a higher standard of first amendment protection.

Searching for anonymous John Does takes a lot of patience and tenacity. Information received through discovery might open up new possibilities for locating the anonymous speaker. Other subpoenas will lead to dead ends. Just as there is no such thing as a perfect crime, persons who make anonymous online statements make mistakes. These mistakes create a trail of bread crumbs that will lead the diligent doe hunter back to the offender.

Notes

1. Hickey v. St. Martin's Press, Inc., 978 F.Supp. 230, 235 (D.Md. 1997).
2. 47 U.S.C. § 230(c)(1).

3. 18 U.S.C. § 2701 *et seq*.
4. 18 U.S.C. § 2510.
5. 18 U.S.C. § 2701 *et seq*.
6. *https://www.verizon.com/foryoursmallbiz/Unprotected/Common/HTML/BroadBand/BB_DynamicStatic.htm*.
7. *https://www.verizonwireless.com/businessportals/support/faqs/DataServices/faq_static_ip.html*.
8. For a fuller explication of IP addresses *see https://www.eff.org/files/2016/09/22/2016.09.20_final_formatted_ip_address_white_paper.pdf*.
9. Independent Newspapers, Inc. v. Brodie, 966 A.2d 432, 440 (Md. App., 2009).
10. Hard Drive Prods., Inc. v. Doe, 892 F.Supp.2d 334, 338 (D.D.C., 2012).
11. *See* Sinclair v. Tubesocktedd, 596 F.Supp. 2d 128, 132 (D.D.C., 2009).
12. *Brodie*, 966 A.2d at 456.
13. Dendrite Int'l, Inc. v. Doe, 775 A.2d 756 (App.Div. 2001).
14. Doe v. Cahill, 884, A.2d 451 (Del. 2005).
15. *Brodie*, 966 A.2d 432.
16. *Id*. at 446, 457.
17. In re Subpoena of Daniel Drasin Advanced Career Technologies, Inc. v. John Does 1-10, Civil Action No. ELH-13-1140, 8 (D. Md. 2013).
18. *Id*. at 5.