# The Right to Speak Anonymously Online … and its Limits

BY RICK SANDERS

AARON SANDERS
CREATE • INNOVATE • PROTECT

The business of law isn't usually discussed outside of law firms, and usually not even there. But one business-law trend has everyone's attention. Over the law few years, there has been a push to use lawsuits to monetize heretofore low-value copyrights, such as those in newspaper articles and pornography. The thought is that these properties are undervalued because they are so frequently pirated. These lawsuits differ from the RIAA's campaign against file-sharers, in that the RIAA was trying to deter future infringement, while rights-holders are simply trying to make money—or, as they'd put it, recover lost royalty streams.

Righthaven is probably the best-known example of this business practice, but almost as well-known are the mass lawsuits involving alleged downloading of full-length films over bit-torrent networks. In these cases, a filmmaker will sue several hundred or thousand defendants for downloading the filmmaker's movie over the bit-torrent protocol. Most, but not all, of these cases have been filed in the United States District Court for the District of Columbia (the "D.D.C.") because law firm that pioneered the practice is located near there. These cases were formed by the confluence of two streams: one for mainstream movies (including Oscar-winners like *The Hurt Locker*) and one for pornographic movies (which originally arose in West Virginia, of all places).

The business model is as follows: you sue thousands of defendants in a single case, pay a single $350 filing fee, identify the defendants using legal procedure, then contact the defendant with a relatively small settlement offer. The defendants are usually ordinary consumers without the resources or knowledge to defend themselves. A few thousand dollars looks like a good deal compared to the costs and headaches of a lawsuit. Where the film in question is pornographic, the defendant might be willing to pay little extra to avoid being publicly named in the lawsuit.

The legal model is as follows: By the time the filmmakers are ready to sue, they've found out the IP address of every bit-torrent session involving the film in question. The IP address isn't enough to identify most, if not all, of the defendants. The filmmaker needs information in the possession of the defendants' various ISPs. So the filmmaker files a lawsuit naming the defendants "John Doe," and asks the court for permission to take early discovery for the purpose of obtaining this information. Since there's nobody to object, the judge usually grants permission, and the filmmaker sends subpoenas to the ISPs. Once the identifying information is obtained, the complaint to replace the John Does with actual names. Usually, the ISPs or some of the defendants will object and try to "quash" the subpoenas before the ISPs can turn over the information. Usually, the judge rejects these attempts.

This article uses a decision from over the summer in the most notorious of these cases, *West Coast Productions, Inc. v. Does 1-5829*, to discuss three basic questions: (1) the nature of the right to remain anonymous, (2) the procedure used to iden-

2400 Crestmoor Road, Nashville, TN 37215 • p 615-385-2690 • m 615-482-4038 • rick@aaronsanderslaw.com

tify anonymous defendants, and (3) why the filmmakers in these cases have generally been able to identify the defendants (although the trend has reversed itself in the last few months). *West Coast* is one of the "pornographic" cases, which are thought to be more lucrative because defendants are motivated to avoid being identified. As with most of other bit-torrent cases, some of the defendants tried to block the hand-over of their identifying information, and as in most of those cases, the judge refused to do so.

## Balancing the Right to Anonymity with the Right to Redress

The question is: when can someone aggrieved by something you wrote anonymously online peel back your anonymity and discover your identity—presumably so you can be sued? This comes up in a variety of contexts, but the two most contentious are local (community) "electronic bulletin boards" (including those operated by local newspapers) and national "electronic bulletin boards" and comment threads dedicated to a (usually publicly traded) company. It also comes up in websites critical of a company or products (sometimes known as "sux" websites) and blogs (but again, typically where companies, products or local affairs are involved).

The free-speech concern is that not all victims of anonymous online speech are interested in seeking redress.

Obviously, you can't be sued if you can't be identified, so naturally you'd prefer not to be identified. Less cynically, you might have legitimate reasons to keep people from connecting you with your speech. You might not want to your employer, spouse, neighbors or business associates to know that you hold certain views or engage in certain (otherwise legal) behaviors. The First Amendment right to free speech is supposed to encourage unfettered discussion, and anonymity helps with that.

Turn the issue around, and you could rephrase the question as: when can someone hide behind the cloak of anonymity when his or her online speech violates someone else's rights? Let's say someone posted something to a community forum about you that's both untrue and harmful to your reputation. Or someone has posted confidential financial figures about your business on an online discussion group. How do you go about suing someone whose identity might not even be able to suspect? It might not be enshrined in the Constitution (the Founders didn't seek to enumerate every single right), but you have a pretty ancient right to seek redress for wrongs done to you through the civil courts.

The free-speech concern is that not all victims of anonymous online speech are interested in seeking redress. Some just want the speaker's identity, presumably so they can subject the speaker to some sort of extra-legal retribution, such as firing the speaker, shunning the speaker at the country club or posting one's own dirt about the speaker. From a free-speech point of view, these implied extra-legal threats chill speech, undermining one of the key goals of the First Amendment.

All courts understand the right to seek redress through the courts. That makes sense—it's what courts are for. In addition, many—perhaps most—courts also understand the importance of anonymity to free speech. These courts will seek

to find some way to balance the right to free speech against the right to redress. They typically do this by demanding an additional showing from the plaintiff—perhaps some evidence, or just some additional detail about the claim—to make sure the claim is really viable and that the plaintiff is really serious about the claim. This helps to prevent the worst-case scenario: the speaker's identity is exposed, but the plaintiff loses, so the right to free speech is violated for nothing.

Some courts, though—mostly state courts, but perhaps also including a U.S. Court of Appeals—seem almost to ignore the First Amendment. To them, this is an incredibly simple question. You can't have a lawsuit without a defendant, you can't have a defendant without knowing the defendant's identity, and we have a lawsuit; therefore, the defendant's identity must be revealed.

In sum, we can feel pretty confident that anonymous online speakers have a First Amendment right to their anonymity, and we see that this right must be balanced against the right to obtain redress in court. And it's nice to have such rights—but how do you assert them? How do they play out in practical terms? To understand that, you need to understand how plaintiffs go about trying to learn the identities of anonymous defendants in internet-related cases.

## Legal Trail Through the Internet to You

Let's put these competing rights into some real-world context by discussing the steps the filmmakers in *West Coast* took to learn the identities of the defendants.

The filmmakers found themselves with a pretty typical problem: they knew the IP addresses that were used in carrying out the allegedly wrongful act, but that they weren't enough to identify the actual person. It's usually fairly easy to figure out what IP address was being used at a certain time in connection with a certain activity. There are lots of IP address trackers available for free, and sometimes all you need to do is look it up on an access log.

An IP address is, indeed, a unique identifier—of sorts. It looks something like 150.0.14.201. At any given time you're connected to the internet (in a "session"), your computer or router has a unique IP address. With IP address lookup available for free, you'd think that'd be enough to identify at least the subscriber associated with that number. In the case of large companies with constant "always-on" internet service, that'd be true. They have stable ("static"), assigned IP addresses. But with ordinary consumers, that's not the case. Consumers typically have "dynamic" IP addresses. Consumers' ISPs own large blocks of IP addresses, but not enough for each one of their customers, who aren't going to be all logged in at the same time. When one of their customers starts an internet session, the ISP assigns one of its IP addresses to the customer for that session. When the customer logs in again the next day, chances are he or she will be assigned a different IP address.

This is where the ISP comes into our discussion about anonymous speech. The ISP keeps a log of which customer was assigned which IP address at what time. With this information, it's just a matter of cross-indexing the IP address and the time to determine the subscriber. So if you're a plaintiff in one of these online anonymity cases, the trick is to make the ISP give you this information. At a minimum, this means filing a lawsuit because ISPs aren't going to hand the information over

without legal compulsion—*i.e.*, a civil subpoena—and you normally can't issue a subpoena without filing a lawsuit.

Filing the lawsuit, however, raises something of a paradox because you don't know who your defendants are. Naming the defendant isn't the problem—you can always temporarily name them as "John Doe." The problem is that you don't know where they live. Not all courts have the power to hale a defendant into court and issue an enforceable judgment against the defendant (a concept known as personal jurisdiction). Indeed, when it comes to ordinary consumers, very few courts have such power. Ordinary consumers are usually subject to the jurisdiction of the courts in the consumer's home state and perhaps one or two others where the alleged acts took place. But if you don't know who the defendant is, you probably don't know where the defendant lives, which means that you really don't know where to sue the defendant.

Filing the lawsuit raises something of a paradox because … if you don't know where the defendant leaves, you don't know where to sue the defendant.

ISPs, for their part, display a wide range of attitudes when they receive a civil subpoena seeking their customers' identities. Some will comply unquestioningly, even with facially defective subpoenas, perhaps fussing over timing and cost, but doing almost nothing to protect their customers. Others will hold the plaintiffs' feet to the fire, sometimes going so far as to try to "quash" (block) the subpoena. If you have to deal with the less pliable sort of ISP, you might have a bit of a fight on your hands—and that's just so you can name your defendant.

Once you've obtained the information from the ISP, it ought to be a straightforward matter of cross-indexing to identify the defendants. Since the defendants usually don't do much affirmatively to hide their identities, this shouldn't be a very difficult procedure. And yet, much can, and does, go wrong. For one thing, where there are thousands of IP addresses at issue, some of those addresses are bound to be simply wrong. Numbers get transposed, the IP address tracking program isn't 100% accurate, and the IP address might have been spoofed, and so forth. Even if all that goes perfectly, the subscriber isn't necessarily the guilty party. Other members of the household or building could have done the deed. (It's pretty common for the children to be blamed.) If the subscriber uses an unsecured local network, it may be impossible to know who might have been using the network at a particular time.

But what about that First Amendment right to speak anonymously—where does that come in? It comes in at the subpoena stage. The ISP itself might oppose the subpoena, asserting its customers' rights (and its own rights). If the ISP lets the customer know about the subpoena, the customer can try to intervene anonymously and "quash" the supboena. In either event, the First Amendment will be playing a prominent role.

## Why the Judge's Decision Was Right (but Feels Wrong)

In *West Coast*, several of the anonymous defendants sought to quash the subpoenas issued to their ISPs. They made four main arguments. First,

they argued that they lived outside of Washington D.C., and thus weren't subject to the personal jurisdiction of the court. Second, they said that they have a privacy right not to be identified. Third, they said that the subpoenas were defective and the ISPs shouldn't have responded. Fourth, they said that thousands of defendants are just too many and that they must have been "misjoined" to the lawsuit.

Judge Kollar-Kotelly, who is a very good judge, ruled against the defendants on all counts. She held that she couldn't rule on the personal jurisdiction questions because she doesn't know who the defendant are, so that question was premature (which is how she resolved the catch-22 of how to exercise jurisdiction over anonymous defendants). She further held that the consumers (as opposed to the ISPs) didn't have standing to challenge any defects in the subpoenas. And she held that joinder (*i.e.*, combining many defendants in the same lawsuit) was there to promote judicial efficiency, and at this stage, it's not really that hard to manage a suit with thousands of defendants (but that might change as she learns more about the defendants).

What about the privacy interests? What about free speech? Is Judge Kollar-Kotelly one of those judges who doesn't give the First Amendment enough weight in deciding whether to "out" an anonymous speaker? How could she ignore the well-developed (if fractious) federal caselaw on the subject?

The truth is that this article has been leading you on. *West Coast* and the other bit-torrent cases don't have that much to do with free speech because of what the defendants are being accused of: copyright infringement. The classic case for protecting online anonymity was to encourage robust debate and guard against chilling effects. But, here, the defendants are alleged to have made illegal copies of the filmmakers' movies. There's some expressive content in doing so—you indicate what movies you like and perhaps comment on whether your actions should perhaps be legal—but not much. *See Sony Music Entertainment v. Does*, 326 F. Supp. 2d 556 (S.D.N.Y. 2004). At least, it's not nearly as much as writing, "Mayor Brown is corrupt and I have the photos to prove it!" or even "Growco is going down in flames!"

This made Judge Kollar-Kotelly's decision easy, and correct. The filmmakers get the opportunity to obtain redress from infringers, and the defendants have a chance to defend themselves. Just like any other lawsuit. And yet…

...and yet it doesn't seem entirely fair for those who are mis-identified. Yes, they now have a chance to defend themselves, to show that they aren't the ones who downloaded the movies. But lawsuits, even "slam-dunk" ones, are not cheap for ordinary citizens to defend. You have to pay a lawyer. You are taken away from more immediate work and family tasks to focus on the lawsuit. You have to rummage through your files and computers to respond to "discovery requests." You have to "freeze" the information on your home computer because it's now evidence in the case, and the mere act of using it might cause "spoliation" of evidence. And then there is the gnawing fear in the back of your mind that somehow everything will go wrong and you'll be found liable despite your innocence.

If previous mass-defendant copyright-infringement cases are any guide, there will be hundreds, perhaps thousands, of defendants who have been mis-identified and will have to spend money, time

and sanity to clear their names. Some will cave in and pay a small settlement because it's cheaper and easier. This doesn't seem right.

The answer is not, however, to make it harder to sue anonymous downloaders of copyrighted material. The answer is to make sure that those who are wrongly sued are compensated by the copyright holders, and that the copyright holders are incentivized to be careful at the outset and to drop defendants when it becomes clear that a mistake was made. Right now, there's little downside to a plaintiff if it makes a mistake, or if it persists in a lawsuit when it's clear that the defendant was misidentified. The only thing protecting such defendants is "Rule 11," which is a kind of smell test for new lawsuits. Rule 11 motions are expensive and nasty, and don't work very well in John Doe lawsuits where there's no one to bring the motion. So Rule 11 is not enough. Plaintiffs should be on the hook for their misidentifications, in an amount sufficient to compensate the misidentified parties and also to get the plaintiff's attention.

Right now, there's little downside to a plaintiff if it makes a mistake, or if it persists in a lawsuit when it's clear that the defendant has been misidentified.

The Copyright Act already has a potential mechanism for this: the awarding of a successful defendant's attorney's fees and costs. This will allow defendants to hire lawyers to adequately defend their rights. Since the fees will only increase the more the plaintiff persists, the plaintiff will have an incentive to investigate early, drop obvious mistakes, and work with defendants to obtain correct identifications. For this to work, though, the award has to be pretty much automatic, in cases where a defendant has been misidentified in a mass-defendant case, regardless of the copyright holder's good faith. After all, if you sue 5829 defendants, you can hardly say you were surprised when you learn that you made a few hundred mistakes.

## Post-Script: The Trend May Be Reversing, but Not Because of Free Speech

In another of the D.D.C. bit-torrent cases, *Nu Image, Inc. v. Does 1-23,322*, a different judge disagreed with Judge Kollar-Kotelly's notion that a defendant may be haled into an inappropriate court, so long as she can object at a more appropriate time. When the filmmaker in *Nu Image* asked for permission to take "expedited discovery" for the purpose of obtaining information necessary to identify the John Doe defendants, the judge said no. Usually, these motions are granted because there's no one to object at this early stage—the defendants don't know they've been sued yet. But the judge decided to oppose the motion himself (in a sense) through a "show cause" order, in which he asked the plaintiff to explain to him why it's proper to hale all of these defendants into his court.

In denying the request for expedited discovery, Judge Wilkins' starting point was the uncontroversial point that the plaintiff needed to show "good cause" for the discovery. His twist was that good cause included a showing that there was at least a reasonable chance that the defendants were being properly haled into his court. What are the odds that any one of the 23,322 defendants actually resides in Washington D.C.? Not very high.

The judge didn't throw the case out entirely. He didn't require absolute proof of residency, only a "good faith belief" of residency. That's not a very high standard. In fact, it's low enough that the judge will accept IP-address geolocation services as a reasonable proxy, fully aware of their limitations. He's just looking for some way to cut down substantially on the number of false-positives, *i.e.*, from about 23,000 false positives to maybe 1,000.

It must be emphasized that Judge Wilkins was not concerned about anonymity per se. He probably doesn't disagree with Judge Kollar-Kotelly's main point that there is only a negligible free-speech right in downloading copyrighted materials anonymously. Rather, the judge seemed offended that his court was being used a clearinghouse for identifying tens of thousands of defendants and, by extension, identifying the proper courts for those defendants:

> The Court understands why, for the sake of convenience and expense, the Plaintiff would desire to use this single lawsuit as a vehicle to identify all of the 23,322 alleged infringers. Furthermore, the Court understands and is sympathetic to the need to combat copyright infringement. However, it is not appropriate, and there is not good cause, to take third-party discovery in this case solely to obtain information that will be used in another lawsuit in a different venue. As the Supreme Court has stated, "[i]n deciding whether a request comes within the discovery rules, a court is not required to blind itself to the purpose for which a party seeks information. Thus, when the purpose of a discovery request is to gather information for use in proceedings other than the pending suit, discovery properly is denied." [Citations omitted.]
>
> In addition, the Court must take into account the delay and unproductive utilization of court resources in prosecuting this lawsuit if the Plaintiff is allowed to seek discovery with respect to all 23,322 putative defendants, only to result in the eventual dismissal of the vast majority of those John Does later when it is revealed that they are not District of Columbia residents. The Court would need to govern litigation over motions to quash third-party subpoenas and motions to dismiss relating to hundreds or thousands of putative defendants who cannot be tried in this Court (if they make a motion).

In response to the argument that jurisdiction is a defense that must be asserted (which Judge Kollar-Kotelly found persuasive), Judge Wilkins said that the argument defies common sense. Most of the improperly named defendants would raise the defense, and there's no point waiting around to find out.

The strangest thing about this decision—the thing that must have really stunned the plaintiff's lawyers—is that these lawyers had previously been before Judge Wilkins in nearly identical case, and Judge Wilkins had to this point always granted their request for expedited discovery. What changed the judge's mind?

According to Judge Wilkins, he changed his mind when he figured out what the correct venue statute should be. It's well known that 28 U.S.C. § 1400(a) governs copyright actions. Since copyright actions also invoke federal-question jurisdiction, you'd think that 28 U.S.C. § 1391(b) would

also apply. Section 1391(b) provides that federal-question actions "may, except as provided by law, be brought only in" certain districts. Section 1400(a) provides that copyright actions "may be brought" in certain districts. By a plain reading of the two statutes, you would think that § 1400(a) expands on the venue options provided by § 1391(b).

Judge Wilkins used to think so, but he's changed his mind. He now thinks that, for copyright actions, § 1400(a) is the exclusive venue statute. Section 1391(b) doesn't apply. In his Show Cause Order, he makes a pretty persuasive case. To me, the most persuasive argument is that the Supreme Court has held that § 1400(**b**) is the exclusive venue statute for patent actions. If you swap "copyright" for "patent," § 1400(a) is no different from § 1400(b).

This makes a big difference because § 1400(a) limits venue to only those districts "in which *the* defendant or his agent resides or may be found." By contrast, § 1391(b) allows actions to be brought in any district "in which *any* defendant may be found, if there is no district in which that action may otherwise be brought." In other words, if a single one of the thousands of anonymous defendants lives in Washington D.C., venue is proper. Under § 1400, however, any defendant who is not a resident of Washington D.C. must be dismissed.

Thanks for reading!

RICK SANDERS (RICK@AARONSANDERSLAW.COM) IS A PARTNER AT AARON & SANDERS, PLLC, IN NASHVILLE, TENNESSEE.