BACAL ANDERSEN & GARRISON LAW GROUP

The Masked Internet Villain: What to Do When Your Business Is Attacked on the Internet by Someone Who Has Taken Steps to Shield Their Identity

By David M. Andersen

Maligned or violated on the Internet? What if a friend or colleague calls and tells you about a website that is defaming you or your business, infringing your trademark or copyright rights, or posting your company's confidential or proprietary information online? Upon accessing the website, you may realize that it could inflict serious harm to your business and/or your reputation. But how do you stop this activity? What steps should you take? This article provides an initial roadmap.

Anonymous attacks on the Internet are not uncommon. Courts and juries often take these kinds of attacks very seriously. For example, just this spring, a jury in Texas awarded a couple more than $13 million in damages for defamatory comments made in anonymous posts on a website. Still, as a victim of such an attack, your immediate focus is unlikely to be pursuing litigation and damages. You simply may be wondering how to make this website or these posts go away as soon as possible.

Initially, you are likely to ask, "Who is behind this?" The website itself may not contain sufficient identifying or contact information for the person or group that posted the website. Although you may suspect who might be involved, you need substantive evidence to back up your suspicions. How do you get this information?

The first task is to try to identify the listed registrant, or owner, of the domain name used in connection with the website. This information is available from what is called the WHOIS system. The WHOIS system is used to search databases controlled by domain name registries and registrars, which contain the name and contact information of the listed registrant of a domain name. Numerous websites such as www.whois.net and www.whois-search.com provide a free service that allows anyone to search the WHOIS information to determine the listed registrant of the domain name.

After conducting a WHOIS search for the listed registrant of the domain name, you are likely to discover that the wrongdoer is hiding behind virtual walls. Domain name owners and website operators willing to violate others' rights on the Internet usually do so anonymously by utilizing domain name privacy or proxy services that shield the true owner's identity. The purpose of these services is to keep others from discovering who is behind a particular website. As a result, the WHOIS search is likely to reveal only the name and contact information of the company

providing these domain name privacy or proxy services—either the registrar itself (e.g. GoDaddy or Moniker) or a company focused on providing only proxy services (e.g. Domains by Proxy).

In many instances, where a proxy service is not shielding the identity and contact information of the underlying domain name registrant, you may discover that the information provided in the WHOIS record is inaccurate or incomplete. Occasionally, if the person violating your rights is naïve or does not care about being caught, the WHOIS record may reveal the true identity and contact information of the domain name owner, but this is rare in these kinds of cases. In the vast majority of cases, it is usually not clear from the WHOIS record who the real person or group behind the website is. Fortunately, there are other ways of discovering this information.

Most companies that do offer privacy services shielding the true identity of the domain name registrant also require the registrant to agree not to use those services in violation of others' rights, including uses that are infringing, defamatory, abusive, threatening, or otherwise unlawful. Most hosting companies (those that service the website owner by storing the website's content) have similar terms of service. Many of these services reserve the right in their user agreements to terminate the services or even to disclose the identities of their users if they violate these terms. Still, many of these companies are highly reluctant to provide any information unless required to do so by law. Domain privacy services are particularly loath to provide this information because their business models rely on their ability to keep their customers' identities anonymous.

So, what is your next step in discovering the true identity of the anonymous or shielded registrant? Often, a domain privacy company will accept complaints about rights violations. Companies such as Domains by Proxy often will forward these complaints to the underlying registrant to respond or otherwise defend against the complaint. Sometimes, if the underlying registrant ignores the complaint or is unwilling to change behavior that violates the rights of others, the domain privacy company may reveal the listed identity and contact information to the complaining party.

More commonly, however, domain privacy companies and even hosting companies will require a subpoena before they will provide information about their customers. Even if the domain privacy company reveals identifying and contact information, such a company is unlikely to reveal other information such as payment information without being served with a proper subpoena. A subpoena for production of documents or information must be issued and served in the jurisdiction where the production will occur. For example, a subpoena issued to GoDaddy or Domains by Proxy (both located in Scottsdale, AZ) should be issued through the state or federal courts in Arizona.

Service of a subpoena requires the existence of a pending legal action. If there is an existing case, and the information is discoverable, the subpoena may be issued in that case. In Arizona state court, subpoenas are issued by the clerk of the court in which the case is pending, or a party may secure a subpoena through the online subpoena service provided by the State Bar of Arizona. In federal court, an attorney authorized to practice in that district may issue a subpoena. For proceedings pending outside the United States, federal courts may allow discovery in aid of foreign proceedings, pursuant to 28 U.S.C. § 1782. If there is no action pending, a party may be able to initiate a lawsuit against a "John Doe" defendant and seek to use the discovery procedures, including subpoenas, to identify that defendant and pursue claims against him or her. In any event, if the domain privacy service does not provide information in its possession, a subpoena is likely to be necessary to discover information about the underlying registrant.

Often, discovery of the information listed in the WHOIS database is insufficient to determine who is actually engaged in the unlawful activities. The domain name registrant may have listed inaccurate or incomplete contact and/or identifying information, either publicly or with the domain privacy service. In other words, the domain name privacy service itself may not know the true identity or accurate contact information of the domain name registrant. Nonetheless, even without discovering the true identity of the underlying registrant, there are still means of stopping the unlawful activities, as outlined below.

Once you discover the purported registrant of the domain name or determine that the registrant's true identity is not currently available, competent legal counsel should be able to assist you in identifying how to go about enforcing your rights and obtaining any remedies to which you may be entitled. Before going any further, however, you should identify your end goals. What harm are you trying to prevent? What do you want from your enforcement activities? Answers to those questions will affect the steps and the cost of the steps you will then authorize your attorney to take.

If your goal is simply to prevent use of an infringing domain name, one option is to file an administrative complaint under the Uniform Domain Name Dispute Resolution ("UDRP") procedure. These procedures are governed by rules adopted by the Internet Corporation for Assigned Names and Numbers ("ICANN"), the body that coordinates and controls the domain name system and Internet Protocol ("IP") addresses.

The UDRP allows the infringing domain name to be transferred to a successful complainant, whereas the URS will be a fast means of stopping registration of a clearly infringing domain name. A UDRP proceeding (and likely a URS proceeding) may be filed against the listed registrant of the domain name, even if that registrant is the privacy company itself. The advantage of these administrative procedures is that they generally work on a set time line and therefore are usually less expensive and faster than asserting claims in court.

If controlling or stopping registration of the domain name is insufficient to remedy the problem (e.g. the infringer simply uses a different domain name to post the same website), or if you are seeking other remedies (e.g. damages), you likely will need to go beyond administrative procedures and assert legal claims in court. Such claims might include state law tort claims such as defamation, injurious falsehood, or misappropriation of trade secrets. They also might include federal claims such as trademark infringement or unfair competition under the Lanham Act, cybersquatting under the Anti-Cybersquatting Consumer Protection Act, or copyright infringement under the Copyright Act.

In certain cases, claims may be filed against an anonymous person or even against the domain name itself, which is considered intangible property subject to disposition by a court. Although a court proceeding is far more expensive and time consuming than administrative proceedings, filing claims in court allows you to seek damages and injunctive relief such as a permanent injunction against future violation of rights, which would otherwise be unavailable in an administrative proceeding.

Ultimately, which enforcement mechanisms you decide to use will depend on the projected harm caused and threatened by the website, the resources available to you, and your calculation about the ability of the attacker to withstand a challenge to his or her activities. In some circumstances, a cease- and-desist letter from either your or your lawyer may be sufficient to get the attacker to back off and stop the objected to conduct. In other cases, it may be necessary to initiate available administrative or legal procedures. A step by step approach usually makes sense, trying the

least costly steps first, and hoping that the increased pressure may make the attacker cease the conduct before you have to go through an entire administrative procedure or undertake litigation.

Whatever route you decide to take, it is important that you retain capable and experienced legal counsel with an understanding of all of these available options and procedures. Armed with this knowledge and utilizing a competent attorney in an efficient manner, you should be in a good position to bring to an end any unlawful Internet attack on your business, even where such an attack is mounted by a wrongdoer who has taken steps to shield his or her identity.

Bacal Andersen & Garrison Law Group regularly represents clients regarding a wide range of Internet law matters, including disputes involving anonymous domain name registrants. Glenn Bacal and David Andersen have assisted several clients with Internet and domain name issues under the UDRP, ACPA, Lanham Act, and the Copyright Act. They also have advised clients with respect to new generic top-level domains (gTLDs). With the advent of new gTLDs and the corresponding exponential increase in the number of domain names, intellectual property infringement on the Internet is likely to increase substantially. For more information on this and other related topics, please visit our website at www.bacalgroup.com or contact David Andersen directly at david.andersen@bacalgroup.com or 480-245-6234.