In-House Counsel Guidebook:

How to Handle Internet Defamation and Online Reputation Attacks

VORYS

Higher standards make better lawyers.®

Table of Contents

Introduction

Online reputation attacks have become one of the easiest and most impactful mechanisms for individuals and companies to cause serious damage to businesses.

These types of attacks can originate from a variety of sources, but most commonly the "attackers" are competitors, disgruntled employees, disgruntled customers, disgruntled investors, extortionists or other people and businesses who become upset with a company (or associated individuals) and want to cause that company serious damage.

Further, these attacks come in many forms. Some common types of attacks include making a slew of defamatory postings on gripe websites such as Ripoff Report and Pissed Consumer; posting false information on social media websites or apps, including Facebook and Twitter; anonymously sending defamatory emails to clients or customers; posting false reviews on Yelp or similar websites; altering Wikipedia entries about a company or particular executives in an embarrassing or otherwise harmful way; or creating websites or blogs and posting disparaging information on these platforms. The common misperception is that this conduct is somehow protected. It is not.

Considering the ease with which these types of attacks can be initiated, and because of how quickly content can spread on the internet, online reputation has become a top concern for businesses and executives. In fact, according to "Exploring Strategic Risk," Deloitte's 2013 survey of 300 executives, reputation was cited as the

top strategic risk for large businesses. Not only was it the overall "highest impact risk area," but reputation was also the top concern in most individual sectors. A primary cause for such concern is how easily and quickly information can spread on the internet and social media, and the resulting potential of widespread damage.

Since these types of attacks are becoming so common, and considering the strong First Amendment protections in the United States, businesses are facing serious challenges in protecting and defending themselves against these attacks. Given that a legal analysis is often involved when determining how to handle these online reputation attacks – both against the businesses themselves and their professionals – we expect that in-house legal counsel will commonly be asked for input.

This Guidebook provides a number of insights for in-house counsel involved with these types of situations – based on what we have learned from handling hundreds of these types of cases – and reflects what we believe will be most helpful to in-house counsel dealing with online reputation attacks on their businesses.

The Multi-Disciplinary Approach

The solutions for online reputation attacks are very fact dependent and require analysis from a variety of different disciplines. Especially when in-house counsel does not regularly handle online reputation attack cases, we recommend that the harmed party consult with a multi-disciplinary team to analyze his or her situation (or, at minimum, gather information from non-legal experts with relevant information). In addition to the attorney, a multi-disciplinary team of experts typically would include a cyber investigator, someone experienced in online public relations and/or marketing and a decision maker from the business.

Oftentimes, cyber investigators can find important information about or relating to the attacker. This includes how sophisticated the attackers are, whether they are capable of causing further damage, and how high the negative content will appear in the search engine results over time.

PR and marketing professionals can provide insights into what kind of impact the damaging material will have on the business' online marketing and PR strategies, as well as how they think they can act to mitigate the harm of that same content.

The business decision makers often weigh in on their cultural philosophies on how aggressively they want to respond to the online attacks; the resources they want to dedicate to responding to online attacks; whether they like the type of feedback generated for attention (even if the publicity is negative); or if they simply want to demonstrate they will not tolerate anyone attacking their brands or executives on the internet.

It Takes a Team

We have found that when each of the different experts analyzes a client's dilemma, far better solutions can be developed and implemented than if just one of the experts has individually addressed the particular problem.

By way of example, we were involved with a case in which we consulted with a PR firm and learned the cost of "burying" the harmful material down search engine results was outside the client's budget. However, after analyzing the legal issues involved and given the nature of the offending content, we believed we could ask the court to order the defendant to pay our client for the cost of a corrective online PR campaign. We then conferred with a cyber investigator to determine the identity of the defendant, and it became apparent that the defendant had deep pockets. Based on the collaboration with each of these professionals, we filed a lawsuit on our client's behalf, and our client successfully obtained funds from the defendant for corrective advertising. The client was able to use this money to compensate the PR firm for the corrective advertising necessary to repair the damage from the attack and recover monetary damages from the defendant (more on this technique at the end of the Guidebook).

Moreover, we have seen many businesses make the wrong decisions by relying on a single expert to handle their problems, rather than considering other, more practical options. This reminds us of the "law of the instrument" principle associated with psychologist Abraham Maslow, which involves overreliance on a single tool: "I suppose it is tempting, if the only tool you have is a hammer, to treat

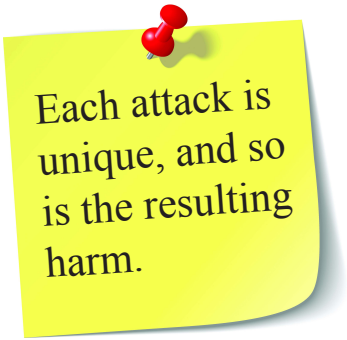
everything as if it were a nail," Maslow was credited with saying in 1966.

We commonly see experts, ignorant of other options and the risks of their own approaches (or simply being more concerned with their own businesses than clients' welfare), only attempting to utilize their own approach when it may not be the appropriate one. For instance, many attorneys will send a cease and desist letter or file a lawsuit that can actually make a situation worse.

In March 2014, an attorney representing a New York business sent such a letter to the author of a critical – but seemingly legitimate – Yelp review. A photograph of the threatening letter soon after surfaced online and the story was widely publicized. Consumers searching the business on Google can now find several news stories about the threatening letter among the top search results.

Similarly, an online PR or marketing professional might advise a company that the company should pay them to "push" the negative material down search engine rankings, when the material might be more easily removed with a court order. However, by the time the company realizes that it is unable to successfully suppress the content in search results, the relevant state's statute of limitations may expire and the court order approach will no longer be available. Utilizing a multi-disciplinary approach can help guard against this problem and ensure the right situation is being developed for the business.

When a multi-disciplinary team analyzes how to respond to an online attack, there are a host of factors that experts must consider, including the potential impact of the attack, the cost of potential solutions, the culture of the business, and the risk of making the situation even worse. Further, each attack is unique, and so is the resulting harm. Some online attacks may be just minor concerns to businesses, whereas others can be extremely detrimental. Thus, when determining the best approach for handing such attacks, it often boils down to a balancing of the potential harm of the online attacks against the costs and risks of responding in a particular manner, as well as the overall likelihood of success of a potential solution.



A business can certainly tell if and to what extent the online attack is damaging its profits. For instance, a business can look at whether there has been a drop in profits since the defamatory posting; it can examine whether other factors have changed which could have caused a decrease in profits; or it can examine if the negative online information was the cause. Aside from traditional financial data, there is other specific information in-house counsel and the business should gather to get a suitable handle on the potential harm of the reputation attack.

Should You Respond?

Among the first factors to consider in terms of how to respond to an online reputation attack are the specific characteristics of the attacker. It will be important to determine whether this is likely a one-time attack by a disgruntled party or the beginning of a full-fledged campaign attack. A cyber investigator can analyze the attacker's behavior, as well as determine how sophisticated he or she is and how likely they might be to spread the information around the internet in highly visible places. Similarly, it is wise to see whether the attacker has a large following or online presence, for instance if he or she manages a blog or has a strong social media presence.

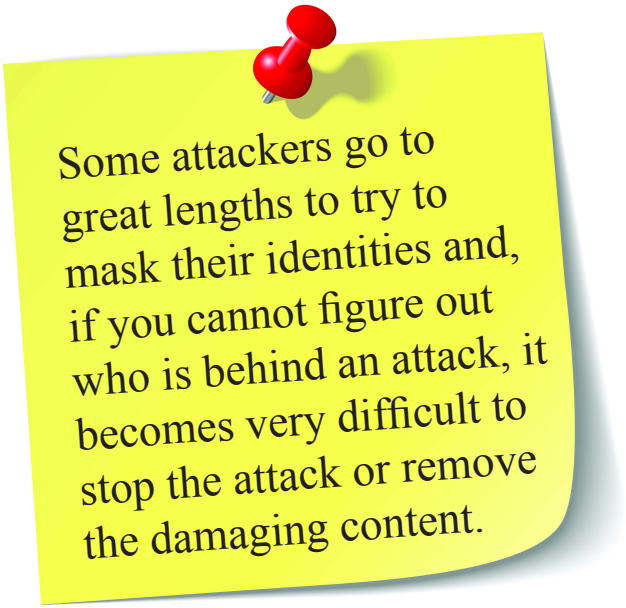
In short, it is important to find out as much information as possible about the attacker and determine if the attacker poses a significant threat to a particular business. Not only will this be helpful in evaluating the potential harm, but also the particular response strategy.

It is important to also consider not just where the information is presently located, but if it has the potential to spread to places that will be seen by larger audiences. This is critical information to evaluate for several reasons, including statute of limitations considerations, as that begins to run the day material is first posted online. Even if the harmful content does not initially rank highly on search engines, it eventually could appear on the first page of search engine results (including after the statute of limitations has expired). Further, at any point a person could hyperlink to the defamatory posting somewhere that will reach a significantly higher number of people searching for your business. Thus, in evaluating the potential harm, in-house counsel should consider the probability that the

information could spread at some point in the future and, if not dealt with, it could leave the harmed party without legal recourse.

Identifying Anonymous Persons

Many online reputation attacks are executed anonymously, so the first step that must be undertaken is identifying the source of the attack. Some attackers go to great lengths to try to mask their identities and, if you cannot figure out who is behind an attack, it becomes very difficult to stop the attack or remove the damaging content. In many cases we have handled, there is no question that the attack was illegal, so the real issue – rather than proving the person(s) violated the law – was to identify who is behind the attack. Of course, many anonymous attackers assume their identities have been shielded, but are ignorant of the fact that through the subpoena process or with the aid of a cyber investigator, it is typically possible to identify attackers.



A. Cyber investigators can successfully obtain the Internet Protocol (IP) addresses of anonymous posters which, in

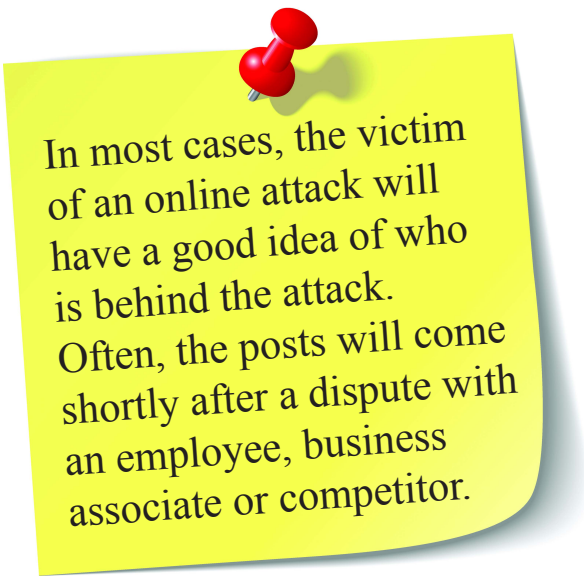
turn, can be used to subpoena the internet service provider for subscriber information associated with the IP address. However, an attorney must ensure the cyber investigator is not creating ethical problems. A primary technique cyber investigators often use is "pre-texting," which involves misrepresenting his or her identity to attempt to get the author of a harmful post to take some action in order to obtain the author's IP address. In most states, if an attorney hires a cyber investigator to do pre-texting, the attorney can be found to have violated that states' ethical rules.

B. Through a subpoena to a third-party website hosting the damaging content, in-house counsel can obtain personally identifying information pertaining to the poster of the harmful content. The full process is fleshed out more in our **Subpoena Guide for Identifying Anonymous Internet Posters**, but, in short, the objective is to obtain personally identifying information from the website and internet service provider (ISP). Once the identity of the attacker is known, the company and attorney can decide how they wish to proceed.

   Many times, since anonymous posters often know better than to disclose any personal information (such as name and personal email address) when registering with a website, the only helpful information received in response to a subpoena is the IP address. Once an IP address is obtained, an attorney can identify the associated internet service provider, such as AT&T or Comcast, through a simple internet search such as on the website: **http://whatismyipaddress.com/ip-lookup**. Once the ISP is identified, an attorney can issue a subpoena

to that ISP for subscriber information associated with that IP address at the particular time(s) and date(s) of the attack(s).

This process is typically effective, but some attackers may use other means to shield their identities. For instance, some attackers use a service to mask their IP address. Alternatively, if someone utilizes a public internet connection to attack your client, such as at a public library or a coffee shop, it can be difficult to identify that customer or patron client. Furthermore, a client and the client's attorney can run into problems identifying the anonymous attacker if the posts are too old, as many ISPs only keep identifying information for a limited time period, such as six months.



In short, the subpoena process is not a simple one. Due to the constitutional protections for anonymous speech in the United States, there are many different factors that can come into play depending on the particular set of circumstances and relevant jurisdiction. Further, each state has its own

rules for issuing subpoenas, and many cases require issuing foreign subpoenas in a jurisdiction outside of the forum state. Thus, it is important in these situations to know the relevant rules in every state in which you plan to issue a subpoena. Moreover, when an attorney issues a subpoena to an ISP when they lack legal grounds for obtaining the anonymous person's identity, he or she may be on the hook for the defendant's legal fees for filing a motion to quash.

C. One of the best tools we have found for determining the identity of anonymous persons online is a forensic exam of suspected attackers' computers. In most cases, the victim of an online attack will have a good idea of who is behind the attack. Often, the posts will come shortly after a dispute with an employee, business associate or competitor. There are often circumstantial facts and even evidence that point to a person behind the posting, though no hard proof. In these situations, a forensic exam can be invaluable. When conducting forensic exams, we have found that the persons behind the attacks will often attempt to "wipe" their electronic devices. However, a forensic exam will obtain fragments that will show the individuals behind the online activity. We have also found it to be common for a poster to immediately use wiping software after they receive notice of our forensic exam. Based on our experience, performing a forensic exam is a very strong tool to prove who posted online attack information when there is circumstantial evidence pointing to someone.

D. Another option when you have a legitimate suspect but cannot prove who is behind the posting is to ask them to

sign a sworn affidavit stating they were not involved in the post. We have found that guilty parties will refuse to sign an affidavit. If they refuse, this provides the victim with at least legitimate grounds to perform a forensic exam of their devices carrying electronic information. Depending on the circumstantial evidence, this may even provide them a sufficient basis to name them as a defendant in a lawsuit.

E. There are a number of cyber harassment statutes in various states around the country under which the police could use their powers to obtain evidence proving who performed online reputation attacks. However, based on our experience, we have found that police rarely devote their resources to brand and reputation attacks on businesses, instead believing these issues are better addressed in the civil court system. Accordingly, under the present system, the police typically do not pursue these cases.

Options for Stopping Attacks, and Removing Damaging Content

Convincing the website to voluntarily remove the harmful content: Most websites have terms of service that very clearly prohibit certain content (e.g. defamatory statements). Each website has its own way of permitting people to report harmful content, and most allow for the removal of the content if it can be shown that the terms or other rules have been violated.

For example, it is a violation of Yelp's Terms of Service and Content Guidelines to write fake or defamatory reviews. Yelp encourages

users to report these reviews and Yelp will consider investigating and taking the appropriate action. Yelp also prohibits a reviewer from publishing an individual's name or other private information "unless you're referring to service providers who are commonly identified by their full names." We have been successful in citing these provisions to convince Yelp to remove certain harmful content.

Wikipedia, meanwhile, has its own deletion procedures to address bad content, including pages solely intended to disparage their subjects. For instance, certain "so obviously inappropriate" content is automatically subject to deletion, whereas other situations require proposing deletion or there being a discussion amongst editors. Additionally, when an article or page conflicts with Wikipedia's policies (such as an article about an executive failing to meet its "Biographies of living persons" standards) an attorney can submit a letter to Wikipedia editors detailing why the article should be removed.

Contacting other media: Another strategy that a company can pursue involves contacting newspapers and other news outlets, and, similarly, asking them to remove damaging material. While each news outlet's policy will vary, we have found that many news organizations will remove outdated information. For example, if a business is charged with a crime or has had a lawsuit filed against it, and that information is published, and then some time after the charge or lawsuit is dropped or resolved favorably for the business, that business can ask the news outlet to remove the outdated articles. This works in a surprising number of cases. In light of the recent European ruling that allows individuals and businesses to petition

Google to have outdated information removed from search results, more domestic websites may be amenable to remove similar information.

Confidential negotiations: In many cases, one of the best strategies is to enter into confidential settlement discussions with the author of disparaging content and negotiating a settlement. This is particularly helpful when an attacker is operating a blog solely dedicated to attacking a company or brand. The best time to pursue this technique is when a company is being severely damaged by the attack but does not want to wait for litigation to resolve the dilemma. Further litigation will likely bring greater exposure that would best be kept out of the public light.

Obtaining court orders to get links to the harmful content de-indexed from search engines: When disparaging content ranks highly on search engines, and when dealing with websites such as Ripoff Report (which refuses to remove any posting, no matter how inaccurate or disparaging its content may be), getting the link removed from Google and other search engines can be extremely helpful. In a nutshell, this process involves filing a lawsuit against the author of the content, obtaining a court order (via judgment or agreements with the defendant(s)), and presenting the court order to the search engine. Although not legally required, **Google typically honors such court orders and will de-index the relevant link**. Thus, the content technically is still online (accessible only by very specific searches on the particular hosting website, such as Ripoff Report), but it would not show up in traditional search results – where most people first gather information about a business.

Sending cease and desist letters: These letters can be highly effective – if there is a good legal basis. Once the identity of the person who posted harmful information is known, in-house counsel can contact them by letter, requesting removal of the information and making them aware that the company is prepared to file a lawsuit (attaching a draft complaint) if they do not stop their attacks of the company online. But there should be legal grounds for threatening to bring a lawsuit, or it could create a public relations nightmare. Legal counsel should ask how the company would be perceived in the court of public opinion – as a bully or as a victim?

Bringing a Lawsuit: In many instances, especially when the harm from an attack is significant, a lawsuit may be the most effective solution. Again, many attacks are anonymous, so lawsuits – often brought under state law – may be initiated as "John Doe" suits. Once the attacker's identity is revealed, they can be named as a defendant. As mentioned, be mindful of the statute of limitations, and it is important to be aware of the different claims – and their respective elements – in the states in which the lawsuit is filed. The elements of defamation claims are similar in all states, but vary some by jurisdiction. The statute of limitations for defamation claims in the vast majority of states is one or two years, but for some it is three years (and just six months for slander cases only in Tennessee). Meanwhile, some states, such as California, have trade libel claims. Again, in-house counsel should be aware of filing a lawsuit (or a premature letter) that can cause more harm than good. This relates to the "Streisand effect" concept, referring to Barbara Streisand's 2003 efforts to suppress photos of her Malibu beach home that backfired and led to even greater publicity.

Be mindful of anti-SLAPP statutes: Many states have passed statutes to combat so-called Strategic Lawsuits Against Public Participation (SLAPP). SLAPP lawsuits are often filed in reaction to criticism, in which a business may wish to silence its critics. Thus, states have passed anti-SLAPP statutes permitting a judge to dismiss frivolous lawsuits filed against those exercising their First Amendment rights. So, prior to filing any lawsuit, a plaintiff should not only should ensure he or she has a legal basis for its claims, but legal counsel should also have evidence prepared to survive an anti-SLAPP motion, such as being able to prove the falsity or defamatory nature of the statements, plus proof of damages.

Competitor Defamation

When a competing business publishes a false review about a competitor online, or a fake review touting their own company, this violates the United States' Lanham Act. The Lanham Act prohibits false advertising by competitors and provides that a business can recover significant damages, including treble damages, disgorgement of the competitors' profits, costs of corrective advertising, and attorney's fees if the publication of the false review is willful – which it overwhelmingly is. 15 U.S. Code § 1117(a).

In a recent Pennsylvania case, a marble and granite installation business sued a competitor after it allegedly discovered that several posts on various product review websites were originating from its competitor's IP address. The competitor attempted to argue: 1) these false reviews, as a matter of law, did not constitute false advertising, and 2) it was not responsible for its own employees' online reviews. But the Court disagreed and held the fake reviews constituted

defamation and trademark infringement, violating the Lanham Act. The Court subsequently denied the competitor's motion to dismiss the case. *NTP Marble, Inc. v. AAA Hellenic Marble, Inc.*, 2012 U.S. Dist. LEXIS 93856 (E.D. Pa. Feb. 24, 2012).

Proving Damages

If an attacker has deep pockets or insurance that could cover them for liability resulting from defamation, there are options for proving damages. Of course, in-house counsel can use traditional methods of using financial data to prove lost profits. When disparaging material cannot be easily removed, you might consider hiring an expert who can estimate the costs of what it would take to remove all of the damaging content posted by the online attacker. In many cases when a business is attacked online, the information can spread so far that it may be difficult to remove, and the best solution may be online reputation management (ORM) tactics to "bury" the content.

Under federal and most state laws, courts have routinely held that a plaintiff is entitled to recover costs incurred in performing various forms of damage control, in response to a defendant's false statements. Applying this principle, there is a strong argument that the victim of damaging content online should be able to be reimbursed by the defendant for expenses paid to an ORM firm to push the harmful information down the search results on Google and other search engines. Typical costs to clean up the damage can range from $50,000 to $125,000 per search term. In many instances, somewhere between 20 and 60 search terms – far beyond the name of the specific person or business – need to be restored.

In the defamation context, if in-house counsel is simply seeking an injunction, he or she can typically meet the damages element by showing the online statements are defamatory per se. These statements are considered so harmful that there is no need to prove the harm. In most states – following the Restatement (Second) of Torts, §§ 570-74, or applying similar principles – damages may be presumed when the following types of statements are attributed to the plaintiff: a criminal offense; a loathsome disease; behavior inconsistent with the ability to lawfully conduct business or properly perform in their trade or profession; or serious sexual misconduct.

Settling on the Optimal Solution

Remember that no two attacks are the same. While some techniques for handling such matters may be used more than others or are typically more effective, there is no blanket solution. The surrounding circumstances will dictate how a company can and should handle an attack. As mentioned, before deciding on the best approach, the affected parties must balance the harm from the attack with the costs and risks of responding in a particular manner, as well as the likelihood of success.

The last thing in-house counsel or any other professional wants is to worsen a company's problem or steer them away from the optimal solution. Thus, considering all the relevant options is a must, and doing so and settling on the appropriate solution will benefit all parties.

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 many aspects of internet 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 Guidebook is for general information purposes and should not be regarded as legal advice. Please contact the author if you want more information or have questions about how these concepts apply to your situation.

About the Firm

The Vorys 18-attorney internet defamation group has unique experience assisting clients who are being damaged on the internet. The group focuses on these cases daily and continually refines their strategies and tactics to best suit their clients. They are often working on dozens of cases across the country at any one time, and are constantly using the most up-to-date technologies and approaches to solve their clients' internet problems.

Vorys was established in 1909 and has grown to be one of the largest Ohio-based law firms with nearly 375 attorneys in seven offices in Columbus, Cincinnati, Cleveland and Akron, Ohio; Washington, D.C.; Houston, Texas; and Pittsburgh, Pennsylvania. Vorys currently ranks as one of the 200 largest law firms in the United States according to *American Lawyer* magazine.