



## 510: Cyber-Smeared & Cyber-Attacks: Protecting Your Company

**Thomas J. Donovan**

*Director*

McLane, Graf, Raulerson & Middleton, P.A.

**Hemanshu Nigam**

*Corporate Attorney, Law and Corporate Affairs*

Microsoft Corporation

**Bradford Weller**

*General Counsel, Vice President of Legal Affairs*

Captiva Software Corporation

## CYBERSMEARS & CYBERATTACKS: PROTECTING YOUR COMPANY

### Introduction

No company wants to learn that its good name or that of a key employee is being attacked by unknown parties on the Internet. Today, most public companies and many private companies face varied threats from individuals using the Internet in ways which harm the businesses or their management. Whether the harmful use appears in a sponsored discussion board or on a special purpose web site, the terms employed for this unwelcome publicity range from the "cybergripe" to the "cybersmear" to the "cyberattack."

The cybergripe typically refers to postings in a customer or shareholder forum in which most of the commentary is negative. The cybersmear refers to more serious cybergripes which are false, defamatory or otherwise actionable. The cyberattack refers to the creation and use of a web site dedicated to disparaging a business. *See*, Jeffrey C. Dodd and Timothy C. Langenkamp, *Strategies for Dealing with Attack Sites in Understanding Electronic Contracting 2003* 335 (Practicing Law Institute 2003). For simplicity, this article will use the term "cybersmear" to encompass the range of negative commentary appearing on the Internet specifically directed against a business. This article will not deal with cruder attempts to misdirect web users away from the web site of a business through various Java programming "cyberjacking" schemes. *See*, Kenneth Sanney, Note, *Cyberjacking, Mousetrapping, and the FTC Act: Are Federal Consumer Protection Laws Helping or Hurting Online Consumers?*, 3 *Vand.J.Ent.L.&Prac.* 221 (2001).

### The Problem – Damaging Attacks By Unknown Assailants

Many web portals such as Yahoo! contain a discussion board as part of their menu of services and information related to public companies. Members of the public can easily join the discussion board through a simple registration process with the web site host. The host will collect at least the e-mail address of the new participant, but may decline to collect the person's name or other information. The new participant will then choose a pseudonym, and all subsequent postings from that person's email address will be identified by that moniker.

Many public company discussion boards sink into a routine of rumors and recriminations. Occasionally, some of these rumors are serious enough to affect the stock price. The poster may be attempting to take advantage of these stock swings on the basis of his or her trading position. Beyond the short term effect on stock prices, some postings may accuse management of assorted misdeeds or criminal acts. They may disparage the business or products of the company. Some may go beyond that to the very personal, accusing a manager of giving sexual favors to advance his or her career, or alleging an affair between two employees. And some postings may divulge sensitive business information, whether it relates to sales strategy, customer names or confidential technical information.

While postings on a discussion board are limited to text messages and perhaps hypertext links, attack web sites (including those using misleading names and other techniques to fool search engines into directing traffic to them) give the author the freedom to post all that and more: entire documents, graphics and images, with resources and links to other web sites that attract a greater audience. The author of such web sites can, for a fee, register directly with a registrar such as register.com and, also for a fee, locate a host for the site. In that case, it may be possible to obtain identifying information about the registrant. However, registrants sometimes submit false information to the registrar. Moreover, some hosts, such as thefreesite.com, offer free web page hosting to members of the public who may not need to provide much information to sign up. These sites, when used to attack a business, can include photographs, images of documents and graphics designed to embarrass a business or its management.

Of course, businesses have dealt with negative publicity for years. The public relations industry under the leadership of Edward L. Bernays emerged almost a century ago out of the need to manage the image of public companies. Negative information about businesses turns up in the print and broadcast media routinely, but except for the largest, most businesses tend to stay out of the media glare. The Internet is different. There is almost no limit upon the amount of information (negative or positive) that can be published about a business. That information is readily searchable and may be archived indefinitely by a search engine. Dodd & Langenkamp, *supra*, at 338. That information is also readily available to anyone, at any time, with a computer and Internet access.

Therefore, within the past ten years business management has been forced to deal with the existence of false, defamatory or secret information about their company that may become suddenly available and exposed to millions of people. While there are many options available to management to help cope with this situation, none is ideal and some entail significant risks for the business. The legal landscape reflects, to some extent, the naiveté of the judiciary about the seriousness of the issue, a lack of legislation dealing with liability of cybersmearers, and an unlevel field of play for businesses.

### **Can Cybersmearing Be Stopped? – Several Approaches**

A manager wishing to stop a cybersmear may assume that a negative posting violates some law. After all, it cannot be right for someone to post some rumor about a company's earnings, especially if it is untrue. And it certainly cannot be right for a poster to allege falsely that he is having an affair with the wife of the president of a public company. See, HealthSouth Corp. v. Krum, No. 98-2812 (Pa.C.P. Centre County). See generally, Scot Wilson, Note, *Corporate Criticism on the Internet: The Fine Line Between Anonymous Speech and Cybersmear*, 29 Pepp.L. Rev. 533, 547-51 (2002). But as any lawyer knows, what is not right may not be actionable. A brief synopsis follows of the types of claims which can arise from a cybersmear.

#### **1. Libel**

The false statement made about the wife of the president of HealthSouth on a Yahoo! Finance bulletin board was libelous because it was both untrue and defamatory. Similar other untrue statements of fact may also be libelous (a human resources vice president "sleeping her

way to the top”). The problem with cybersmears is that they often are not so off the wall or so unrelated to the company’s business. For instance, any discussion board posting stating that the CEO is incompetent, that the company’s products are lousy or that its stock price is due for a fall, would likely be considered a matter of opinion, not fact. And opinions on matters of public concern are protected by a qualified First Amendment privilege. See, e.g., *Milkovich v. Lorain Journal Co.*, 497 U.S. 1 (1990). See also, Lyrissa B. Lidsky, *Silencing John Doe: Defamation & Discourse in Cyberspace*, 49 *Duke.L.J.* 855, 919-944 (2000). One judge has opined that virtually every statement posted on internet discussion boards, because of the very nature of the media and a perception of the absence of credibility, is therefore protected opinion. Global Telemedia, Inc. v. Does 1-25, 132 F.Supp.2d 1261 (C.D.Cal. 2001) (court’s opinion focused mostly on outlandish messages like “you are one of the stupidest suckers who ever posted here” and the response “[you are] a degenerate who speaks regularly from his lower orifice.”). Even statements of fact cast as parody are exempt from libel claims. Beyond that, most publicly traded companies are likely to be considered public figures as to their business activities, which requires the companies to prove, like a politician, that the libeling defendant acted with actual malice. Lidsky, *supra*, at 907-912.

Apart from the opinion and public figure hurdles, most trial lawyers agree that any libel case is difficult to prove and therefore to win. Except perhaps to obtain recompense for very personal false statements appearing on the web, the result may not be worth the cost. See, Thomas G. Ciarlone, Jr. and Eric W. Wiechmann, *Cybersmear May be Coming to a Website Near You: A Primer for Corporate Victims*, 70 *Def.Couns.J.* 51, 51-52,62 (2003)(discusses well-known Varian Medical Systems libel litigation in California which resulted in a substantial libel verdict in 2001 against cybersmearers, but which did not stop negative web postings. For instance, former employees posted over 14,000 messages alleging that Varian’s management videotaped public bathrooms, then created a negative web site about the company.) Lidsky, *supra*, at 872-76 and n. 96 (citing statistics that “public figure” corporations win libel cases only five percent of the time).

## 2. Unfair Trade Practices/Business Disparagement

Some states, like Texas, recognize a tort of business disparagement, similar to the tort of “injurious falsehood”. *Dodd & Langenkamp, supra*, at 340-341. See also, Restatement (Second) of Torts § 623A. Other states have versions of so-called little Federal Trade Commission Acts which prohibit false advertising and unfair competition, and provide private causes of action for damages and injunctive relief. See, e.g., Ill.Comp.Stat. Ann. 505/1-12; Mass.Rev.Stat. Ch. 93-A; Colo.Rev.Stat. §§ 6-1-101-15. See also similar uniform acts found in 7A U.L.A. 69,139. But in the case of business disparagement, the same libel hurdles of malice and falsity will apply. In the case of unfair competition statutes, the defendant must normally be engaged in commerce, i.e. a competitor, and not merely a complaining customer, employee or stockholder.

Under federal law, Section 43(a) of the Lanham Act, 15 USC § 1125(a), prohibits false or deceptive advertising about another’s product, and allows damages and injunctive relief. But it is designed to deal with competitive situations, and not consumers or others who have a gripe with a company. Wojnarowicz v. American Family Association, 745 F.Supp. 130 (S.D.N.Y. 1990). See, *Dodd & Langenkamp, supra*, at 342-43.

### 3. Securities Laws

To the extent a cybersmearer makes a statement which adversely affects a company's stock price, that person could be liable to a stockholder for securities fraud under Rule 10(b)(5) of the Securities Exchange Commission ("SEC") issued pursuant to Section 10(b) of the Securities Exchange Act, 15 USC § 78j(b). Ciarlone & Wiechman, *supra*, at 59-60. While the plaintiff stockholder litigation bar normally looks for deeper pockets than might be the case with a cybersmearer, there is some risk that stockholders may bring claims against managers who fail to stop cybersmears that depress a stock price.

Those who regularly participate in discussion boards of publicly traded corporations appear to be obsessed with the notion of market manipulation. The "pump and dumpers" square off against the "bashers" and the "shorts" in profanity ridden diatribes about a company's virtues and flaws. There is a common perception that the "shorts" (i.e. "short sellers") often hire proxies to post endless negative comments about a target company, particularly in response to anyone saying anything positive. They do so with the hope that the market price of the stock in these companies will be driven down, enabling the "shorts" to cover and to profit. While the SEC has occasionally expressed concern about this phenomenon, it has taken little action in this area. The SEC has focused almost exclusively on the public companies, alleging that the companies themselves are disclosing inaccurate or incomplete information on discussion boards to inflate their own stock prices.

### 4. Copyright

An attack web site often will seek to use rope provided by its target to perform the hanging of the business to be cybersmeared. Whether it be material from its annual report or internal memoranda, a business may find much of its documentation posted on a web site for all the world to see, perhaps to ridicule or even to profit from. The material may be as simple as a photo of the president or it may be as complex as the source code of the company's main software product.

In this case, the copyright owner has a claim for injunctive relief and money damages against the infringer under the Copyright Act, 17 USC § 101 *et seq.* Registration with the Copyright Office is not a prerequisite to ownership, although registration even after the fact will increase the remedies available to the business plaintiff. 17 USC § 412. *See*, Dodd & Langenkamp, *supra*, at 346-48.

### 5. Trademark

The relationship of federal trademark law (Lanham Act, 15 USC § 1051 *et seq.*) to cybersmears is very close, since the name and other marks owned by a business are the bulls eye of the target for the cybersmearer. From the creation of web sites with the domain name [yourbusiness]sucks.com to the use of company logos in obscene or uncomplimentary ways, the Internet provides many opportunities for mischief and harm around a company's marks.

For the [yourbusiness]sucks.com web site, there has been a cottage industry of litigation and commentary on this phenomenon. The recent decision in *Taubman Co. v. Webfeats*, 319 F.3d 770 (6<sup>th</sup> Cir. 2003) ruled in a fact-intensive case that because the defendant's

“taubmansucks.com” site was purely an exhibition of free speech and was not “in connection with the sale ... of goods” (15 USC § 1114(1)), there was no violation of the Lanham Act. Id., 319 F.3d at 777-78. In fact, the Court held that “although economic damage might be an intended effect of [defendant’s] expression, the First Amendment protects critical commentary when there is no confusion as to source, even when it involves the criticism of a business”. Id. But see, People for the Ethical Treatment of Animals v. Doughney, 263 F.3d 359 (4<sup>th</sup> Cir. 2001) (injunction granted against parody site “peta.org” where found to be in connection with the sale of goods); Planned Parenthood Fed’n of America, Inc. v. Bucci, 152 F.3d 920 (2d Cir. 1998) (injunction granted where likelihood of confusion found after pro-life group acquired “plannedparenthood.com” domain name).

Of course, Congress has also passed the Anticybersquatting Consumer Protection Act, 15 USC § 1125(d)(1)(A), which forbids use of a confusingly similar domain name with the intent to profit from the same. That provision would not seem to help businesses facing an obviously negative domain name, such as those with the “sucks” suffix. Cf., People, supra; Rita A. Rodin et. al, *Enforcing Your Trademark Rights under the UDRP and the ACPA in Trademark Law and the Internet: Challenges of the Digital Age*, 201,203 (Practicing Law Institute 2002). And while the Uniform Domain Name Dispute Resolution Policy is a quicker and cheaper administrative remedy for trademark holders seeking the transfer of confusingly similar domain names, its panels also tend to uphold web site names that clearly express criticism of a business. *Id.* at 210-211.

Of course, attack web sites can use trademarked names as metatags or as purchased search engine key words to direct search engine users to a particular site. Such usage of a registered trademark has been found to create initial interest confusion. See, e.g. Eli Lilly & Co. v. Natural Answers, Inc., 233 F.3d 456 (7<sup>th</sup> Cir. 2000)(use of “Prozac” metatag for the web site of an herbal remedy alternative). See, Rodin et al., supra, at 220-24.

An attack web site can also contain numerous hyperlinks to pornographic sites, to sites selling products or even to sites of competitors of the attacked business. Where the links are to commercial sites, the commerce link to the Lanham Act is made. Thus if a web site which criticizes a business by name also creates links to a competitor, that may constitute trademark infringement because it makes commercial use of the trademarked name. See, Bihari v. Gross, 119 F.Supp.2d 309 (S.D.N.Y. 2000). If the mark is famous, there is also an argument that the hyperlink causes trademark dilution by tarnishment, prohibited by the Federal Trademark Dilution Act, 15 USC § 1125(c). See, Martha Kelley, Note, Is Liability Just a Link Away? Trademark Dilution By Tarnishment Under the Federal Trademark Dilution Act of 1995 and Hyperlinks on the World Wide Web, 9 J. Intell.Prop.L. 361 (2002). Of course, trademark dilution under the FTDA just got harder, since the Supreme Court ruled in Moseley v. V Secret Catalogue, Inc., 537 U.S. 418 (2003) that a plaintiff has to show “actual injury” to the value of its famous trademark in order to make out a dilution claim.

## 6. Trade Secrets

Most states have enacted some form of the Uniform Trade Secrets Act, 14 U.L.A. 433 (1990), which affords businesses with strong injunctive and damages remedies against persons who misappropriate a trade secret by acquisition or disclosure. A typical cybersmearer is a

disgruntled former employee who obtains and posts technical or commercial trade secret information which the former employee received on the job and which was subject to appropriate confidentiality controls. When the employee left, he or she absconded with a copy of this information, and is using it to cause embarrassment or economic harm to the company. See, MCSi, Inc. v. Woods, 2003 U.S. Dist. LEXIS 3086 (N.D. Cal. 2003) (misappropriation of trade secrets alleged in postings on Yahoo! discussion board).

The major issue in trade secret litigation typically concerns whether the information is a trade secret. It requires findings that there is both independent economic value from its secrecy and reasonable efforts to maintain that status. Internal financial records can be a trade secret as well as technical materials. In cybersmear litigation, obviously only that portion of the negative material that is a trade secret can be enjoined through this statute. Still, the statute does provide a powerful remedy for a portion of what may get posted on a discussion board or on a web site.

## 7. Contracts

Many a cybersmearer is a disgruntled former employee. That employee may remain subject to an employment or similar agreement containing some form of a confidentiality or nondisparagement or noncompetition clause. Those agreements may also explicitly reference injunctive relief as well as money damages remedies against former employees who violate the terms. Noncompetition provisions may be difficult or impossible to enforce. But confidentiality provisions are more typically enforced against former employees, typically for those who held responsible positions with a business.

A business may even attempt by contract to limit its customer's public statements critical of its products. But such provisions have backfired on a seller requiring it. See, People v. Network Associates, Inc. d/b/a McAfee Software, No. 400590/02 (N.Y. Sup. 1/6/03) (provision held to be a deceptive trade practice). *Dodd & Langenkamp, supra*, at n.71.

## 8. Property Torts

Some lawyers are dusting off intentional torts involving property rights and using them for internet-related offenses. In *Kremen v. Cohen*, 2003 U.S. App. LEXIS 14830 (9<sup>th</sup> Cir. 2003), the court held that the theft of a domain name constituted conversion, even though the right was intangible. However, in *Intel Corp. v. Hamidi*, 71 P.3<sup>rd</sup> 296 (Cal. 2003), the California Supreme Court found no trespass to chattels from the actions of Intel ex-employees sending thousands of negative emails to current Intel employees at their place of work. Thus, to the extent that a cybersmearer actually "invades" a company's cyberspace, either through massive attacks on its server or through appropriation of its domain name or addresses, there may be a cause of action.

## 9. Terms of Service

Most every discussion board or web site host requires participants to mouse click their agreement with specific terms of service for use of the board or site. Those terms typically include provisions prohibiting scandalous matter or in violation of the intellectual property rights of another. They also give the host the discretion to remove material or terminate the rights of a contributor. *Ciarlone & Wiechmann, supra*, at 62. See, excerpts from Yahoo! Terms of Service, attached as Exhibit 1.

A business that is victimized by a cybersmear certainly can contact the host to request that it exercise its discretion to enforce its terms of service against a cybersmearer. These hosts will often cooperate by removing offensive material. Ciarlone & Wiechmann, *supra*, at 62. But the business does not have a cause of action against the host, because Section 230 of the Communications Decency Act, 47 USC § 230 (“CDA”) has been interpreted to give immunity to internet service providers with respect to the content of materials appearing on their sites. See, e.g., *Zeran v. America Online, Inc.*, 129 F.3d 327 (4<sup>th</sup> Cir. 1997). But see, *Batzel v. Smith*, 333 F.3d 1018 (9<sup>th</sup> Cir. 2003) (analyzing whether listserv moderator is covered by CDA § 230); Paul Ehrlich, Comment, *Communications Decency Act § 230*, 17 Berkeley Tech.L.J. 401 (2002)(arguing that § 230 does not provide total immunity).

## **Procedural Roadblocks to Pursuing the Cybersmearer**

As discussed in the previous section, there are several possible legal claims that a business may make against a cybersmearer, which could result in injunctive relief or damages. Those causes of action have, built within them, certain defenses which can make it difficult for a business to succeed with such a claim. For instance, libel claims come with public figure and opinion speech defense, and trademark claims require proof of a commercial use of a protected mark. But there are other legal hurdles facing businesses in pursuit of these claims, and those are discussed in this section.

### **1. Anonymity**

Most discussion board participants use a pseudonym. Their identity is hidden to other users of the board, and the host may have little more identifying information beyond an e-mail address. The identity of the owner of an attack web site may be more public, unless it is operated as a web page hosted by a third party. In order to get relief against the cybersmearer, eventually the business needs to uncover the identity of that person. Obtaining that identity is often as difficult as winning the case on the merits.

In the cybersmear context, businesses have often resorted to naming “John Doe” as defendants in litigation, coupled with expedited discovery requests (subpoenas) aimed at the third party web host to obtain the identity of the poster or web page owner. This process is not ideal, since a John Doe leaves personal or subject matter jurisdiction issues unsolved for the court. Particularly federal courts are hostile to John Doe defendants. See, *Bryant v. Ford Motor Co.*, 844 F.2d 602,605 (9<sup>th</sup> Cir. 1987); Megan M. Sunkel, Note, *And the I(SP)S Have It ... But How Does One Get It? Examining the Lack of Standards for Ruling on Subpoenas Seeking to Reveal the Identity of Anonymous Internet Users in Claims of Online Defamation*, 81 N.C.L.Rev. 1189, 1200-07 (2003).

One alternative available in some states is to bring a discovery action directly against the third party host, seeking in that action only the identity of the cybersmearer. See, exhibit 2, attached. Such litigation may be available against the host, even if it is immune from liability under the CDA. In this way, an employer is immune from suit in the worker’s compensation context, but may be sued by an employee solely to discover what manufacturer made the machine on which the employee was injured. See, *Robbins v. Kalwall Corp.*, 417 A.2d 4 (NH 1980).



A second alternative is available where there is an allegation of copyright infringement. There is a subpoena provision in the Digital Millennium Copyright Act, 17 USC § 512(h) ("DMCA") which permits a copyright owner to subpoena an internet service provider to produce the identity of a person using infringing material on its site. The owner must apply to the federal court for issuance of a subpoena, accompanied by a declaration that there is an infringing use of copyrighted material. A sample application and subpoena is attached as Exhibit 3. The constitutionality of this provision has been upheld twice recently in In re Verizon Internet Services, Inc., No. 03-MS-0040(JDB) (D.D.C. 4/24/03) and No. 02-MS-0323(JDB) (D.D.C. 1/24/03), 240 F.Supp. 24 (D.D.C. 2003). The ACLU, Yahoo! and some other ISPs are joining this issue with Verizon, and this battle is not over.

While Verizon is engaged in appeals to avoid turning over to the Recording Industry Association of America information about DSL subscribers (and music downloaders), *id.*, many web hosts do not fight third party subpoenas. In fact, their terms of service, discussed earlier, tell users not to expect anonymity in the face of subpoenas. Joshua L. Furman, *Cybersmear or Cyber-SLAPP: Analyzing Defamation Suits Against Online John Does as Strategic Lawsuits against Public Participation*, 25 Seattle U.L. Rev. 213,230-33 (2001); Wilson, *supra*, at n. 18; Ciarlone & Wiechmann, *supra*, at 62.

Most of the reported cases seeking discovery to determine the identities of cybersmearers discuss whether the anonymity of the poster is protected by the First Amendment. Courts and commentators have waxed eloquent on the important free speech values contained in anonymous speech, citing the Supreme Court's decision reaffirming the importance of preserving the anonymity of unsigned political leaflets, McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995). As a result, a number of state and federal judges have refused to issue subpoenas upon web hosts to disclose the identities of cybersmearers. Some of these cases may take McIntyre too far, and some courts have seemed to be carried away with free speech values at the expense of the value of permitting the victims of cybersmeas to litigate their cases. See generally, Caroline E. Strickland, Note, *Applying McIntyre v. Ohio Elections Commission to Anonymous Speech on the Internet and the Discovery of John Doe's Identity*, 58 Wash.&Lee L.Rev. 1537,1571-85 (2001).

Courts have created multi-part tests to weigh the interests of the anonymous poster against those of the business that has been cybersmeared. The first major articulation of such a test occurred in Columbia Insurance Co. v. Seescandy.com, 185 F.R.D. 573 (N.D.Cal. 1999), a trademark infringement case involving an anonymous poster. The court created a four factor test, which was later adopted by a New Jersey appellate court. Dendrite Int'l, Inc. v. John Doe, 775 A.2d 756 (N.J.Super.Ct.App. 2001). The four requirements are: 1) enough identity of the unknown defendant to determine jurisdiction; 2) an attempt to locate and serve the unknown party; 3) proof that the underlying action would survive a motion to dismiss; and 4) a discovery request specifically geared to complete service of process. Columbia, 185 F.R.D. at 579-80. Other cases considering subpoenas to locate the identities of cybersmearers are collected in Sunkel, *supra*, at 1207-1213.

## 2. Anti-SLAPP Statutes

A number of states have passed legislation designed to prevent businesses from filing lawsuits to intimidate citizens fighting real estate development or other corporate activities. Those lawsuits became known as Strategic Lawsuits Against Public Participation (“SLAPP”), and they found the wrath of legislators around the country. Foremost among them is California’s statute, Cal.Civ.Proc.Code § 425.16, which requires plaintiffs claiming damages based upon a defendant’s statements to survive a special motion to strike. To go to trial, the court must rule that the plaintiff has a “probability that he or she will prevail on the claim”. This seems to create a separate constitutional issue for the plaintiff, whose jury trial right on disputed factual issues may be infringed by the court’s preliminary ruling. See, Opinion of the Justices (SLAPP Suit Procedure), 641 A.2d 1012 (N.H. 1994)(advisory opinion holding proposed state legislation unconstitutional based upon special motion to strike procedure). Nevertheless, a number of states have enacted Anti-SLAPP statutes. See, e.g., Fla.Stat. Ann. § 768.295; Mass.G.L.A. ch.231, § 59H; N.Y.C.P.L.R. § 3211(g). Activist groups like the California Anti-SLAPP project ([www.casp.net](http://www.casp.net)) are ready for war on behalf of cybersmearers using these statutes.

In Cybersmear cases, the Anti-SLAPP statutes may prevent the disclosure of anonymous posters and lead to obtain the dismissal of lawsuits against those posters complete with an award of attorneys fees. See, Batzel, supra, (statute may be applied in conjunction with CDA § 230), ComputerXpress Inc. v. Jackson, 113 Cal.Rptr.2d 625 (Cal.App. 2001)(statute applied to portion of claims, attorneys’ fees awarded); Global Telemedia (statute applied); MCSi, Inc., supra (statute not applied); Furman, supra, at 245-48 (arguing that Anti-SLAPP statutes rather than First Amendment should be the primary defense against cybersmear lawsuits).

Companies seeking to stop cybersmeas in anti-SLAPP jurisdictions need to consider the significant risks associated with using the judicial system to protect its interests.

## 3. First Amendment

The obstacles to pursuit of cybersmearers, at their core contain First Amendment values. These values show up substantially in the application of the law of libel and trademark. They show up procedurally in the denials of discovery to uncover anonymous discussion board posters. But that same First Amendment might not help a business that tries to correct the record publicly against a cybersmearer. In Kasky v. Nike, Inc., 45 P.2d 343 (Cal. 2002), cert. dismissed as improvidently granted, 123 S.Ct. 2554 (2003), the California Supreme Court let proceed to trial an unfair trade practice case brought by a citizen against Nike because of allegedly false and misleading publicity it put forth as its argument concerning working conditions in its third world factories. While that case is not over, it could have a chilling effect on companies wishing to forcefully correct the diatribe of a cybersmearer. In an ironic twist, the company which defends itself could then get sued by the cybersmearers.

### Realistic Alternatives

Given the uncertain terrain over which cybersmearers must be pursued, what should a business do when facing an attack? Strategies depend upon the particular facts of the attack, the risk tolerance of the company, and the legal landscape in the state.

## 1. Preventive Measures

Many companies buy up derogatory variations of their trade names, including those with the “sucks” suffix, to prevent others from acquiring them. Good confidentiality and nondisparagement provisions in employment agreements are essential to provide a disincentive to former employees from starting to cybersmear. Some businesses have even made nondisparagement or confidentiality a term of an agreement with a customer for the sale of its products.

Beyond that, businesses should monitor discussion boards or web sites dealing with their companies. *Wilson, supra*, at 575-76. They may be able to identify and stop cybersmearers earlier, before damage has occurred to the company.

## 2. Non-litigation

Usually, the first task for a business is to locate the identity of the cybersmearer. For an attack web site, theoretically a business can track its owner and the internet service provider hosting the site. Registered owners can be found on WHOIS, but unfortunately much false information is on file. There are tools to discover internet protocol addresses of web sites to locate its host, and its internet service provider. Attached as Exhibit 4 is a primer of basic investigation techniques. Unfortunately, this tool will not lead to the identity of a discussion board poster on a third party's web site, such as Yahoo!.

If by self help, subpoena or self-revelation, the cybersmearer's identity becomes known, the business can send out a cease and desist letter. Sometimes those letters have the desired effect. Also, the company may contact the customer service representative of the web host and request that the offensive postings or poster be removed from the site. Companies like Yahoo! may well comply with such requests voluntarily.

The company may decide to join the fray by arranging for corrective information to show up on its web site or in the discussion boards. Such a move could succeed or backfire, and should be considered with top notch public relations expertise. Moreover, some corrective information may be called for under securities law so that cybersmears do not mislead investors in public companies. *Id.* at 576-77. But, as mentioned before, posting corrective information then poses the risk of an unfair trade practices lawsuit from someone alleging that the business' rebuttal is false. See, *Kasky, supra*.

## 3. Litigation

The most coveted information for the business is the name of the cybersmearer. Many cases end after the identity of the person responsible has been uncovered. Why? Experience shows that a well placed cease and desist letter or court complaint can quiet the cybersmearer. See, *Lidsky, supra*, at 875-83. But to get that information takes a subpoena to a web host. If there is any copyrighted material involved, a subpoena pursuant to the DMCA can be readily obtained. Outside of that, a business may wish to seek a subpoena in a jurisdiction (not New Jersey or California) that is less enamored with the free speech rights of anonymous cybersmearers and which does not have a strict Anti-SLAPP statute. Where direct discovery actions are permitted against the web host, that should be considered as well.

If the company then wishes to pursue its litigation claims, those based upon trade secrets or confidentiality agreements seem less imbued with the free speech concerns of, say, trademark and libel claims. But in any event, the company should exercise some discretion, unless it wishes to end up like Varian Medical Systems, with a substantial judgment but with continuing negative publicity. Or even worse, the company the company bringing the suit against cybersmearers could end up like ITEX Corp., which brought such a suit, only to result in a subsequent SEC suit against it for securities fraud. Wilson, *supra*, at 579-80.

\* \* \* \* \*

## EXHIBIT 1

## 1. ACCEPTANCE OF TERMS

Welcome to Yahoo!. Yahoo! provides its service to you, subject to the following Terms of Service ("TOS"), which may be updated by us from time to time without notice to you. You can review the most current version of the TOS at any time at: <http://docs.yahoo.com/info/terms/>. In addition, when using particular Yahoo! services, you and Yahoo! shall be subject to any posted guidelines or rules applicable to such services which may be posted from time to time. All such guidelines or rules (including but not limited to our Spam Policy) are hereby incorporated by reference into the TOS. If you are a homesteader on Yahoo!'s GeoCities Service, please note that Yahoo! provides a different Terms of Service for you. If you are a member of SBC Yahoo! Dial or SBC Yahoo! DSL, please note that a different ISP Terms of Service applies to you. If you are an account holder through Yahoo! Plus, please note that a different Yahoo! Plus Terms of Service applies to you. Yahoo! also may offer other services from time to time, such as Yahoo! Store and Yahoo! Site that are governed by different Terms of Services. These TOS do not apply to the Yahoo! GeoCities Service, Yahoo! Store or Yahoo! Site or such other services.

## 4. YAHOO! PRIVACY POLICY

Registration Data and certain other information about you is subject to our Privacy Policy. For more information, see our full privacy policy at <http://privacy.yahoo.com/>, or if you came from Yahoo!igans!, then see our Yahoo!igans! privacy policy at <http://www.yahoo!igans.com/docs/privacy/>.

## “Privacy Policy Excerpt”

## INFORMATION SHARING AND DISCLOSURE

- Yahoo! does not rent, sell, or share personal information about you with other people or nonaffiliated companies except to provide products or services you've requested, when we have your permission, or under the following circumstances:
  - We provide the information to trusted partners who work on behalf of or with Yahoo! under confidentiality agreements. These companies may use your personal information to help Yahoo! communicate with you about offers from Yahoo! and our marketing partners. However, these companies do not have any independent right to share this information.
  - We have a parent's permission to share the information if the user is a child under age 13. Parents have the option of allowing Yahoo! to collect and use their child's information without consenting to Yahoo! sharing of this information with people and companies who may use this information for their own purposes;

- We respond to subpoenas, court orders, or legal process, or to establish or exercise our legal rights or defend against legal claims;
- We believe it is necessary to share information in order to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of Yahoo!'s terms of use, or as otherwise required by law.
- We transfer information about you if Yahoo! is acquired by or merged with another company. In this event, Yahoo! will notify you before information about you is transferred and becomes subject to a different privacy policy.
- Yahoo! displays targeted advertisements based on personal information. Advertisers (including ad serving companies) may assume that people who interact with, view, or click on targeted ads meet the targeting criteria - for example, women ages 18-24 from a particular geographic area.
  - Yahoo! does not provide any personal information to the advertiser when you interact with or view a targeted ad. However, by interacting with or viewing an ad you are consenting to the possibility that the advertiser will make the assumption that you meet the targeting criteria used to display the ad.
  - Yahoo! advertisers include financial service providers (such as banks, insurance agents, stock brokers and mortgage lenders) and non-financial companies (such as stores, airlines, and software companies).

\* \* \* \* \*

## 6. MEMBER CONDUCT

You understand that all information, data, text, software, music, sound, photographs, graphics, video, messages or other materials ("Content"), whether publicly posted or privately transmitted, are the sole responsibility of the person from which such Content originated. This means that you, and not Yahoo!, are entirely responsible for all Content that you upload, post, email, transmit or otherwise make available via the Service. Yahoo! does not control the Content posted via the Service and, as such, does not guarantee the accuracy, integrity or quality of such Content. You understand that by using the Service, you may be exposed to Content that is offensive, indecent or objectionable. Under no circumstances will Yahoo! be liable in any way for any Content, including, but not limited to, for any errors or omissions in any Content, or for any loss or damage of any kind incurred as a result of the use of any Content posted, emailed, transmitted or otherwise made available via the Service.

You agree to not use the Service to:

- a. upload, post, email, transmit or otherwise make available any Content that is unlawful, harmful, threatening, abusive, harassing, tortious, defamatory, vulgar, obscene, libelous, invasive of another's privacy, hateful, or racially, ethnically or otherwise objectionable;
- b. harm minors in any way;
- c. impersonate any person or entity, including, but not limited to, a Yahoo! official, forum

- leader, guide or host, or falsely state or otherwise misrepresent your affiliation with a person or entity;
- d. forge headers or otherwise manipulate identifiers in order to disguise the origin of any Content transmitted through the Service;
  - e. upload, post, email, transmit or otherwise make available any Content that you do not have a right to make available under any law or under contractual or fiduciary relationships (such as inside information, proprietary and confidential information learned or disclosed as part of employment relationships or under nondisclosure agreements);
  - f. upload, post, email, transmit or otherwise make available any Content that infringes any patent, trademark, trade secret, copyright or other proprietary rights ("Rights") of any party;
  - g. upload, post, email, transmit or otherwise make available any unsolicited or unauthorized advertising, promotional materials, "junk mail," "spam," "chain letters," "pyramid schemes," or any other form of solicitation, except in those areas (such as shopping rooms) that are designated for such purpose (please read our complete Spam Policy);
  - h. upload, post, email, transmit or otherwise make available any material that contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment;
  - i. disrupt the normal flow of dialogue, cause a screen to "scroll" faster than other users of the Service are able to type, or otherwise act in a manner that negatively affects other users' ability to engage in real time exchanges;
  - j. interfere with or disrupt the Service or servers or networks connected to the Service, or disobey any requirements, procedures, policies or regulations of networks connected to the Service;
  - k. intentionally or unintentionally violate any applicable local, state, national or international law, including, but not limited to, regulations promulgated by the U.S. Securities and Exchange Commission, any rules of any national or other securities exchange, including, without limitation, the New York Stock Exchange, the American Stock Exchange or the NASDAQ, and any regulations having the force of law;
  - l. "stalk" or otherwise harass another; or
  - m. collect or store personal data about other users.

You acknowledge that Yahoo! does not pre-screen Content, but that Yahoo! and its designees shall have the right (but not the obligation) in their sole discretion to refuse or move any Content that is available via the Service. Without limiting the foregoing, Yahoo! and its designees shall have the right to remove any Content that violates the TOS or is otherwise objectionable. You agree that you must evaluate, and bear all risks associated with, the use of any Content, including any reliance on the accuracy, completeness, or usefulness of such Content. In this regard, you acknowledge that you may not rely on any Content created by Yahoo! or submitted to Yahoo!, including without limitation information in Yahoo! Message Boards, Yahoo! Clubs, and in all other parts of the Service.

You acknowledge and agree that Yahoo! may preserve Content and may also disclose Content if required to do so by law or in the good faith belief that such preservation or disclosure is reasonably necessary to: (a) comply with legal process; (b) enforce the TOS; (c) respond to claims that any Content violates the rights of third-parties; or (d) protect the rights, property, or personal safety of Yahoo!, its users and the public.

You understand that the technical processing and transmission of the Service, including your Content, may involve (a) transmissions over various networks; and (b) changes to conform and adapt to technical requirements of connecting networks or devices.

### 13. TERMINATION

You agree that Yahoo! may, under certain circumstances and without prior notice, immediately terminate your Yahoo! account, any associated email address, and access to the Service. Cause for such termination shall include, but not be limited to, (a) breaches or violations of the TOS or other incorporated agreements or guidelines, (b) requests by law enforcement or other government agencies, (c) a request by you (self-initiated account deletions), (d) discontinuance or material modification to the Service (or any part thereof), (e) unexpected technical issues or problems, and (f) extended periods of inactivity. Termination of your Yahoo! account includes (a) removal of access to all offerings within the Service, including but not limited to Yahoo! Mail, Groups, Messenger, Chat, Domains, Personals, Auctions, Message Boards, Greetings, Alerts and Games, (b) deletion of your password and all related information, files and content associated with or inside your account (or any part thereof), and (c) barring further use of the Service. Further, you agree that all terminations for cause shall be made in Yahoo!'s sole discretion and that Yahoo! shall not be liable to you or any third-party for any termination of your account, any associated email address, or access to the Service.

### 23. COPYRIGHTS and COPYRIGHT AGENTS

Yahoo! respects the intellectual property of others, and we ask our users to do the same. If you believe that your work has been copied in a way that constitutes copyright infringement, or your intellectual property rights have been otherwise violated, please provide Yahoo!'s Copyright Agent the following information:

1. an electronic or physical signature of the person authorized to act on behalf of the owner of the copyright or other intellectual property interest;
2. a description of the copyrighted work or other intellectual property that you claim has been infringed;
3. a description of where the material that you claim is infringing is located on the site;
4. your address, telephone number, and email address;
5. a statement by you that you have a good faith belief that the disputed use is not authorized by the copyright owner, its agent, or the law;
6. a statement by you, made under penalty of perjury, that the above information in your Notice is accurate and that you are the copyright or intellectual property owner or authorized to act on the copyright or intellectual property owner's behalf.



Yahoo!'s Agent for Notice of claims of copyright or other intellectual property infringement can be reached as follows:

By mail:

Anthony P. Coll  
Copyright Agent  
c/o Yahoo! Inc.

701 First Avenue

Sunnyvale, CA 94089

By phone: (408) 349-5080

By email: [copyright@yahoo-inc.com](mailto:copyright@yahoo-inc.com)

#### 24. GENERAL INFORMATION

The TOS constitute the entire agreement between you and Yahoo! and govern your use of the Service, superceding any prior agreements between you and Yahoo!. You also may be subject to additional terms and conditions that may apply when you use affiliate services, third-party content or third-party software. The TOS and the relationship between you and Yahoo! shall be governed by the laws of the State of California without regard to its conflict of law provisions. You and Yahoo! agree to submit to the personal and exclusive jurisdiction of the courts located within the county of Santa Clara, California. The failure of Yahoo! to exercise or enforce any right or provision of the TOS shall not constitute a waiver of such right or provision. If any provision of the TOS is found by a court of competent jurisdiction to be invalid, the parties nevertheless agree that the court should endeavor to give effect to the parties' intentions as reflected in the provision, and the other provisions of the TOS remain in full force and effect. You agree that regardless of any statute or law to the contrary, any claim or cause of action arising out of or related to use of the Service or the TOS must be filed within one (1) year after such claim or cause of action arose or be forever barred.

The section titles in the TOS are for convenience only and have no legal or contractual effect.

#### 25. VIOLATIONS

Please report any violations of the TOS to our [Customer Care](#) group.

## EXHIBIT 4

## Cyber-Smeared & Cyber-Attacks: Protecting Your Company Basic Online Investigation Techniques

### Introduction

*Where in the world is that Internet site located? Who is responsible for that site?*

These are the most frequently asked questions when your company is presented with a cyber-smear or cyber-attack. Dealing with Internet cases can be frustrating and time consuming, as technical issues and determining jurisdiction can always delay a decision on whether a case can or should be pursued. The purpose of this document is to allow you and your in-house personnel to take control without spending precious dollars on Internet specialists until you really need to. Below you will find an introduction to Internet terminologies and online tools that will aid you during the course of your investigation.

### Internet Basics

#### Introduction to IP Addressing

An Internet Protocol (IP) address is a set of numbers assigned to a user, or a website, creating a physical presence on the Internet usually in the form of a dotted quad:

#### Some of Microsoft.com's IP Addresses are:

**207.46.249.190**  
**207.46.249.222**  
**207.46.249.27**  
**207.46.134.155**  
**207.46.134.190**  
**207.46.134.222**

Everyone with a presence on the Internet has an IP address assigned to them since a location must be established on where information will be sent to or received from. Thus, all websites have an IP address assigned to them which gives them presence on the Internet and allows the user to retrieve (view) the data that is on that site.

Think of an IP address as your home mailing address, where you need an address for your house in order to receive packages. Without an IP address, no one can find you and the user can retrieve the data on your website.

A domain ([www.something.com](http://www.something.com)) can have more than one IP address, however this is dependent on how much traffic the domain receives and if a request is made by the owner to the ISP hosting the site for several IP addresses.

Thus, it is critical that you know the IP address of any website that you want to investigate.

### Tools To Aid In Your Investigation

- **NSLOOKUP** or Name Server lookup is a very handy tool used in determining an IP address of a domain. One of Microsoft.com's IP addresses is 207.46.249.190, but we would never know it without NSLOOKUP. The reason why domain names exist is because we would never be able to remember all the various IP addresses that exist on the Internet, as humans have a hard time remembering more than 7 digits.

**To perform a NSLOOKUP, simply use the NSLOOKUP tool highlighted below and enter the domain name in question.**

<http://network-tools.com/nslook/> ---- For query type, choose A -Address

- **Reverse NSLOOKUP:** Reverse NSLOOKUP is utilized on an IP address instead of a domain name, to reveal the identity of an IP address in question. For example, performing a NSLOOKUP on 207.46.249.191 reveals the domain name of Microsoft.com. Note that this only works if a domain name is assigned to that IP address, as quite a few websites utilize IP addresses only.

**To perform a Reverse NSLOOKUP, simply use the NSLOOKUP tool highlighted below and enter the IP address in question.**

<http://www.webmaster-toolkit.com/ns-lookup.shtml>

- **Traceroute:** Traceroute is used to verify what part of the country or world a person or server is in. It is also used to determine the latency of a website.

**To perform a traceroute, simply use the traceroute tool highlighted below and enter the domain name or IP address in question.**

<http://www.visualware.com/visualroute/livedemo.html>

- **Ping:** The most generic command of an investigation, the ping command is used to verify if an IP address or a website is still alive.

**To perform a ping, simply use the Ping tool highlighted below and enter the domain name or IP address in question.**

<http://www.webmaster-toolkit.com/ping.shtml>

- **WHOIS:** WHOIS will tell you who is the registered owner of a site in question and the ISP that is hosting the site. *The WHOIS utility is not really an accurate reflection of the registrant information on file, as anyone can falsify or change their WHOIS record after the domain is registered.*

**To perform a WHOIS, simply use the WHOIS tool highlighted below and enter the domain name in question.**

<http://www.internic.net/whois.html>

## WHOIS Accuracy:

**Falsified or inaccurate WHOIS information is a common problem that you may be able to overcome.**

The Internet Coalition for the Assignment of Names and Numbers (ICANN) has a policy that WhoIs data must be accurate. Once notified of the false/inaccurate information, the owner of the registered domain will often require the registrant to provide accurate WhoIs information or face deletion of the domain. A deleted domain means that site will no longer be accessible on the Internet via its domain name. Note that registrars will have different interpretations on the policy.

### *Section 3.7.8 states:*

3.7.8 Registrar shall abide by any specifications or policies established according to Section 4 requiring reasonable and commercially practicable (a) verification, at the time of registration, of contact information associated with a Registered Name sponsored by Registrar or (b) periodic re-verification of such information. Registrar shall, upon notification by any person of an inaccuracy in the contact information associated with a Registered Name sponsored by Registrar, take reasonable steps to investigate that claimed inaccuracy. In the event Registrar learns of inaccurate contact information associated with a Registered Name it sponsors, it shall take reasonable steps to correct that inaccuracy.

<http://www.icann.org/registrars/ra-agreement-17may01.htm>

## Regional Internet Registries

IP address space is distributed in a hierarchical way. IANA (Internet Assigned Numbers Authority IANA.org) allocates blocks of IP address space to Regional Internet Registries (RIRs). RIRs allocate blocks of IP address space to local Internet registries that assign the addresses to end users.

A frequently asked question concerning IP addresses: *“What if I do not have a domain name, but just an IP address, and I have already performed a traceroute and such, but I still do not know where the server is located?”*

Well, a good place to start is by visiting the ARIN (*American Registry for Internet Numbers, Region: North America, Africa south of the equator, and portions of the Caribbean*) website at [www.arin.net](http://www.arin.net). Next, perform a WHOIS on the ARIN database before performing a traceroute, as traceroutes can be hampered by firewalls. Performing a WHOIS on this

database will tell you who owns or is subletting an IP block, thus giving you the location and jurisdiction of the server in question.

Utilizing the ARIN database is rather easy, as explained in the example below:

For this experiment, we will use one of Microsoft.com's IP addresses as an example:

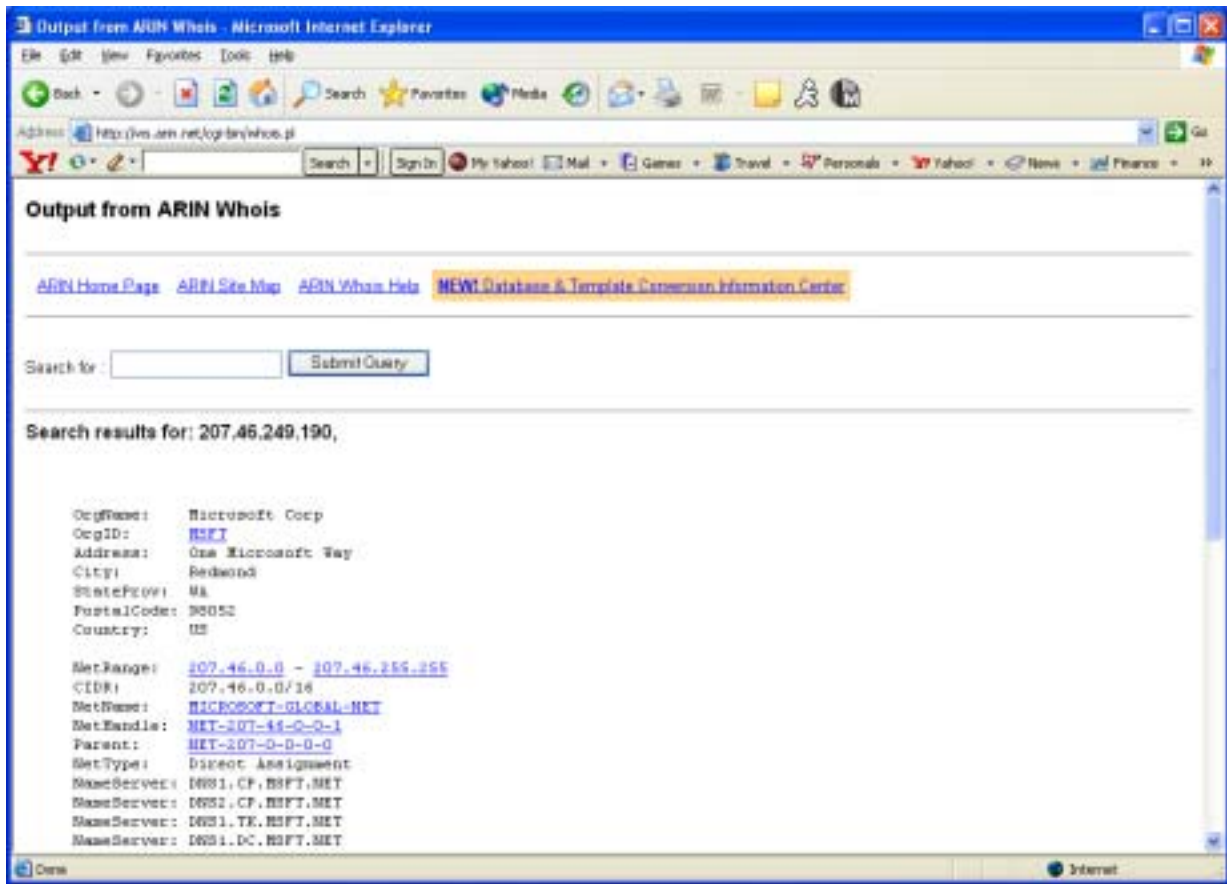
First we will perform an NSLOOKUP to reveal Microsoft.com's IP address:

**207.46.249.190**

Then we take the IP address of 207.46.249.190 and plug it into the SEARCH WHOIS box on the http://www.arin.net homepage (see screenshot below):



We then click on SEARCH WHOIS and get the following results:



The detailed output from the ARIN WHOIS reveals the following:

**Search results for: 207.46.249.190,**

OrgName: Microsoft Corp  
 OrgID: [MSFT](#)  
 Address: One Microsoft Way  
 City: Redmond  
 StateProv: WA  
 PostalCode: 98052  
 Country: US

NetRange: [207.46.0.0 - 207.46.255.255](#)  
 CIDR: 207.46.0.0/16  
 NetName: [MICROSOFT-GLOBAL-NET](#)  
 NetHandle: [NET-207-46-0-0-1](#)  
 Parent: [NET-207-0-0-0-0](#)  
 NetType: Direct Assignment  
 NameServer: DNS1.CP.MSFT.NET

NameServer: DNS2.CP.MSFT.NET  
NameServer: DNS1.TK.MSFT.NET  
NameServer: DNS1.DC.MSFT.NET  
NameServer: DNS1.SJ.MSFT.NET  
Comment:  
RegDate: 1997-03-31  
Updated: 2002-12-05

TechHandle: [ZM39-ARIN](#)  
TechName: Microsoft  
TechPhone: +1-425-936-4200  
TechEmail: noc@microsoft.com

OrgAbuseHandle: [ABUSE231-ARIN](#)  
OrgAbuseName: Abuse  
OrgAbusePhone: +1-425-882-8080  
OrgAbuseEmail: abuse@microsoft.com

OrgNOCHandle: [ZM23-ARIN](#)  
OrgNOCName: Microsoft Corporation  
OrgNOCPhone: +1-425-882-8080  
OrgNOCEmail: noc@microsoft.com

OrgTechHandle: [MSFTP-ARIN](#)  
OrgTechName: MSFT-POC  
OrgTechPhone: +1-425-882-8080  
OrgTechEmail: iprrms@microsoft.com

# ARIN WHOIS database, last updated 2003-07-29 09:24  
# Enter ? for additional hints on searching ARIN's WHOIS database.

From this detailed report, we can surmise that this IP address originates in the United States, in Redmond, Washington. We also can state that any IP address that falls under the following range of [207.46.0.0](#) - [207.46.255.255](#) belongs to Microsoft Corporation. We also have the contact information, as in this case, an email address and telephone number.

Another frequently asked question concerning the ARIN database would be:

*“What if I don't know that the IP address I have is American based, which RIR would I choose?”*

It doesn't matter, as all of these databases are connected to one another. Let's say the IP address that you have originates in Russia, but you were unaware of this. All you would need to do is start with ARIN, plug in the IP address information, and ARIN would link you to the correct registry, which in this case would be RIPE, which would then yield you the correct record for the IP address in question.

### Other RIR's

- LACNIC - Latin American and Caribbean Internet Addresses Registry  
*Region: Latin America and portions of the Caribbean*  
[www.lacnic.net](http://www.lacnic.net)
- APNIC - Asia Pacific Network Information Centre  
*Region: Asia and Pacific region*  
[www.apnic.net](http://www.apnic.net)
- RIPE – Réseaux IP Européens  
*Region: Europe, Parts of Asia, Africa north of the equator, and the Middle East*  
[www.ripe.net](http://www.ripe.net)

### Exercises

**Exercise #1:** Using the tools, outlined below, perform a PING, NSLOOKUP, Reverse NSLOOKUP, TRACEROUTE, and WHOIS on Microsoft.com.

#### **Ping**

<http://www.webmaster-toolkit.com/ping.shtml>

#### **NSLOOKUP:**

#### **Reverse NSLOOKUP:**

<http://www.webmaster-toolkit.com/ns-lookup.shtml>

#### **Traceroute:**

Visual Traceroute with a geographical map:

<http://www.visualware.com/visualroute/livedemo.html>

#### **Whois**

<http://www.internic.net/whois.html>

**Exercise #2:** Using the knowledge that you have attained from the previous exercise, please use the ARIN database to perform a WHOIS search on the IP address for Hotmail.com.



EXHIBIT 2

SERVICE COPY                      STATE OF NEW HAMPSHIRE  
HILLSBOROUGH-NORTH COUNTY                      SUPERIOR COURT

ORDER OF NOTICE - EXPEDITED HEARING

NO. 99-E-0358

WPI Group, Inc. v. Home Page.com, Inc.

FILING DATE: 9/01/1999

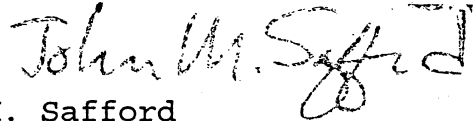
HEARING DATE: 10/19/1999

An original Pleading, a true copy of which is attached, has been filed with this Court at the address of the Clerk stated below. It is therefore ORDERED as follows:

1. WPI Group, Inc. shall cause true copies of the attached Pleading, this Order of Notice and any Orders made ex parte to be served, in a manner allowed by law, upon HomePage.com, Inc. no later than Fourteen (14) days prior to the above hearing date and shall promptly file proof and return(s) of service with this Court; otherwise, this action may be discontinued without further notice.
2. HomePage.com, Inc. shall file a written appearance with this Court at the address stated below on or before the above Hearing Date, and shall cause true copies of such appearance to be delivered to the party or parties bringing this action, or their attorney if represented by an attorney.
3. All parties shall appear before this Court for hearing on the attached Pleading at the Superior Court in Manchester on October 19, 1999 at 9:00 AM.  
Time allotted for this hearing: 30 min.
4. Any party who fails to file a written appearance as required above, or who fails to appear when scheduled before this Court, may be subject to the issuance of such order as the Court may find fair and just from the evidence and argument presented at hearing.

Please advise clients, witnesses, and others that it is a class B felony to carry a firearm or other deadly weapon as defined in RSA 625:11,V in a courtroom or area used by a court.

BY ORDER OF THE SUPERIOR COURT  
9/07/1999

  
John M. Safford  
300 Chestnut Street, Room 127  
Manchester, NH 03101-2490  
603-669-7410

STATE OF NEW HAMPSHIRE

HILLSBOROUGH, SS.  
NORTHERN DIVISION

SUPERIOR COURT

WPI Group, Inc.

v.

HomePage.com, Inc.

**PETITION FOR DISCOVERY**

NOW COMES WPI Group, Inc. ("WPI"), by and through its attorneys, McLane, Graf, Raulerson & Middleton, Professional Association, and petitions this Court to order HomePage.com, Inc. ("HomePage.com") to produce all documents that identify the persons responsible for registering the domain name "wpigroup" and posting information libelous of WPI on HomePage.com's website. In support thereof, WPI states as follows:

1. WPI is a publicly traded New Hampshire corporation with a principal place of business at [REDACTED]. WPI's chairman and chief executive officer is Michael Foster.
2. "WPI Group" is a trade name protected under state and federal law. WPI has registered, and uses, the domain name "wpigroup.com" for its Internet website. A copy of WPI's website homepage is attached as Exhibit A.
3. HomePage.com is an Internet service provider located at 130 West Union Street, Pasadena, California 91103. Through HomePage.com, individuals can register domain names. HomePage.com will host websites developed by its subscribers at the registered domain name.
4. On August 18, 1999, WPI discovered that HomePage.com had registered the domain name "wpigroup.homepage.com" without WPI's authorization and in direct

violation of WPI's property rights. As a result of the registration of the domain name "wpigroup.homepage.com," individuals searching the Internet for WPI's website are directed to HomePage.com's "wpigroup" website, even though this website is not the official website of WPI Group, Inc.

5. WPI also discovered that HomePage.com's "wpigroup" website contained an unauthorized photograph of WPI's chairman and chief executive officer, [REDACTED], as well as statements libelous to him and to WPI.

6. On August 19, 1999, WPI requested that HomePage.com immediately cease and desist from any further use of the domain name "wpigroup" and that it reveal the identity of the persons registering the domain name "wpigroup" and the libelous statements relating to [REDACTED] and WPI. See Exhibit B, August 19, 1999 letter from Mr. Donovan to HomePage.com.

7. Within hours of receiving the cease and desist letter, see Exhibit B, HomePage.com subsequently removed the content of the "wpigroup" website, but it has refused to identify the individuals who registered and posted information to it. See Exhibit C, August 20, 1999 e-mail message from Ms. Porter to Mr. Donovan.

8. In order to pursue its legal rights relating to this libelous and unauthorized website, WPI must first obtain the identity of the persons who registered the domain name "wpigroup.com" with HomePage.com. WPI brings this Petition to compel HomePage.com to release all information within its possession, custody or control relating to the correct names and addresses of all persons responsible for registering the name "wpigroup" and for posting the libelous information on the web page maintained by HomePage.com. WPI does not seek money damages in association with this Petition.

9. This Court is authorized to compel the disclosure of such information pursuant to RSA 498:1, which grants the Court jurisdiction over discovery and in cases in which there is not a plain, adequate and complete remedy at law. In addition, it is established in New Hampshire that "[t]he trial court has ample power to set appropriate time, place, manner and scope of restrictions on non-party discovery whether or not a suit is pending." Robbins v. Kalwall Corporation, 120 N.H. 451, 453 (1980); see also Lefebvre v. Somersworth Shoe Company, 93 N.H. 354, 357-58 (1945)("in some instances discovery will lie against one not himself liable in the main action, to discover facts peculiarly within his knowledge as a result of his dealings with the real or prospective defendants," citing 27 C.J.S. 16).

10. In this case, the identity of the individuals responsible for the "wpigroup" website is peculiarly within HomePage.com's knowledge, and thus it is appropriate for the Court to compel production of this information. Moreover, given the limited nature of WPI's request, the Court can establish appropriate restrictions on the scope and manner of discovery.

11. For these reasons, WPI requests that the Court order HomePage.com to produce any and all records within its possession, custody or control relating to the identity of the individuals responsible for registering the website "wpigroup" and posting materials to it.

WHEREFORE, WPI respectfully requests that the Court:

- A. Grant WPI's Petition for Discovery;
- B. Order HomePage.com to disclose any and all records that reveal the correct name and address of the individuals who registered the domain name

"wpigroup.homepage.com" and of any individuals who posted information to that website;

- C. Schedule a hearing on this matter if any objection to this Petition is filed;
- and
- D. Grant such other and further relief as may be just and equitable.

Respectfully submitted,

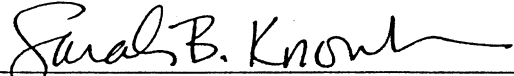
WPI GROUP, INC.

By its Attorneys,

McLANE, GRAF, RAULERSON &  
MIDDLETON,  
PROFESSIONAL ASSOCIATION

Date: September 1, 1999

By:

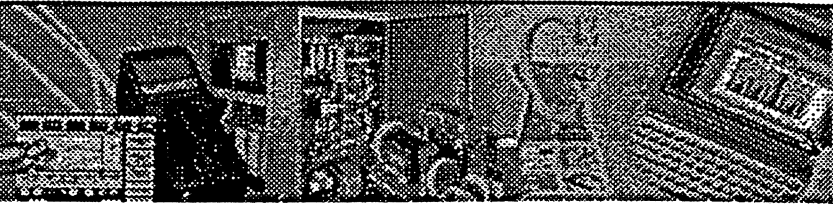


Thomas J. Donovan  
Sarah B. Knowlton  
900 Elm Street, P.O. Box 326  
Manchester, New Hampshire 03105  
Telephone (603) 625-6464



**GROUP, INC.**

*The WPI Family of Companies*



**About WPI Group**

- Company Overview
- Contact Information
- WPI News Bureau

**WPI Products and Services**

- INFORMATION SOLUTIONS GROUP
- INDUSTRIAL TECHNOLOGY GROUP
- WPI Partners

**Career Corner**

- Opportunities
- Our Locations — Profiles
- Fax Back Profile Form

**Investor Center**

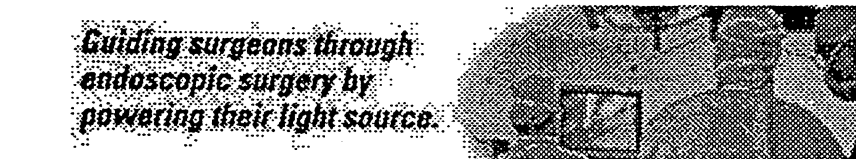
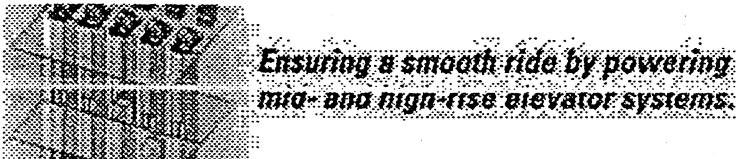
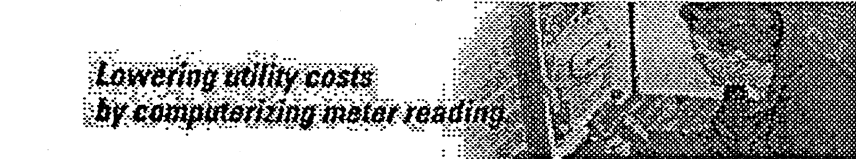
- Stock Quote
- Annual & Quarterly Reports
- Financial Information

**Site Map**

[Legal Notice](#)

• [Second Quarter 1999 Report](#) • [Home](#) •

## Our Products Are With You Every Day



*The fact that you don't know we're there...*

# McLane

McLane, Graf,  
Raulerson &  
Middleton

*Professional Association*

NINE HUNDRED ELM STREET • P.O. BOX 326 • MANCHESTER, NH 03105-0326  
TELEPHONE (603) 625-6464 • FACSIMILE (603) 625-5650

THOMAS J. DONOVAN  
(603) 628-1337  
tdonovan@mclane.com

OFFICES IN:  
MANCHESTER  
CONCORD  
PORTSMOUTH  
NASHUA

August 19, 1999

Via Facsimile: 626-535-2701  
and U.S. First Class Mail

Copyright Agent  
HomePage.com, Inc.  
130 West Union Street  
Pasadena, CA 91103

Re: [www.wpigroup.homepage.com](http://www.wpigroup.homepage.com)

Dear Copyright Agent:

This firm represents WPI Group, Inc., a publicly traded New Hampshire corporation listed on NASDAQ. It is an international technology-based company with subsidiaries in various locations in the United States and abroad. Its chairman and chief executive officer is Michael Foster. WPI's domain name is [www.wpigroup.com](http://www.wpigroup.com).

My client was shocked to discover yesterday that HomePage.com, Inc. has registered the second level domain name "wpigroup" to someone not authorized by WPI Group, Inc. and directly in violation of WPI Group, Inc.'s property rights. It also creates the metatag "WPI Group," which will attract search engine "hits" from inquiries about WPI Group, Inc. Moreover, the content of HomePage.com, Inc.'s web page, [wpigroup.homepage.com](http://wpigroup.homepage.com), contains the unauthorized photograph of WPI Group, Inc.'s chairman and chief executive officer, as well as statements libelous to him and to WPI Group, Inc.

I have reviewed the terms of service under which HomePage.com, Inc. offers its members the opportunity to post web pages using HomePage.com, Inc.'s server. Those terms of service prohibit posting on member web pages, among other things, libelous material, impersonation of an entity, violation of state or federal laws, and infringement of the proprietary rights of any party. The terms of service also purport to absolve HomePage.com, Inc. from responsibility for the content of these web pages. That language may attempt to protect HomePage.com, Inc. from liability for the internal content of a web page, but it certainly can not

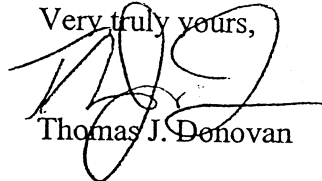
August 19, 1999  
Page 2

protect HomePage.com, Inc. from registering a web page name which violates the property rights of an entity, such as WPI Group, Inc.

This letter demands that HomePage.com, Inc. cease and desist from registration and publication of both the web page name, wpigroup.homepage.com and any related metatag, as well as from continued publication of the deceptive and libelous statements contained on that web page. I will monitor the website for the next 24 hours. If this offensive material and the unauthorized use of the WPI Group, Inc. name is not removed by that time, my clients have authorized me to seek a temporary restraining order to stop this behavior. This web page violates a number of state and federal statutes, including the Lanham Act and New Hampshire's unfair business practices statute. If this material is not removed, WPI Group, Inc. will also seek money damages against HomePage.com, Inc. WPI Group, Inc. also demands that you provide the correct name and address of any persons responsible for registering the name wpigroup or posting the libelous information on that web page.

I look forward to your response today.

Very truly yours,



Thomas J. Donovan

TJD

cc: Michael B. Tule, Esq.

50828



**From:** Debby Porter <debby@homepagecorp.com> at internet  
**Sent:** Friday, August 20, 1999 2:01 PM  
**To:** DONOVAN TOM  
**Subject:** Infringement of Propriety Rights

Dear Mr. Donovan:

In accordance with our privacy policy which is set forth on our website, we do not disclose personal information obtained in our sign-up and registration process. Thank you.

Debby Porter  
Customer Service Manager  
HomePage.com, Inc.

ACCA's 2003 ANNUAL MEETING

CHARTING A NEW COURSE

Issued by the  
UNITED STATES DISTRICT COURT

CENTRAL

DISTRICT OF

CALIFORNIA

ISSUED PURSUANT TO 17 U.S.C. §512(h)

SUBPOENA IN A CIVIL CASE

In re: WPI Group, Inc.

CASE NUMBER: <sup>1</sup>

District of New Hampshire

No. MC-99-33-B

Copyright Agent  
HomePage.com, Inc.

TO: 130 West Union Street  
Pasadena, CA 91103

YOU ARE COMMANDED to appear in the United States District Court at the place, date, and time specified below to testify in the above case.

PLACE OF TESTIMONY	COURTROOM
	DATE AND TIME

YOU ARE COMMANDED to appear at the place, date, and time specified below to testify at the taking of a deposition in the above case.

PLACE OF DEPOSITION	DATE AND TIME
---------------------	---------------

YOU ARE COMMANDED to produce and permit inspection and copying of the following documents or objects at the place, date, and time specified below (list documents or objects):

Pursuant to 17 U.S.C. §512(h), the name(s), address(es) and all other identifying information (such as internet protocol codes) concerning all persons or entities who had anything to do with the registration, ownership or the content of the worldwide web page wpigroup.homepage.com.

PLACE McLane, Graf, Raulerson & Middleton, Attn: Thomas J. Donovan 900 Elm St., Box 326 Manchester, NH 03105	DATE AND TIME 10:00 AM October 12, 1999
---	---

YOU ARE COMMANDED to permit inspection of the following premises at the date and time specified below.

PREMISES	DATE AND TIME
----------	---------------

Any organization not a party to this suit that is subpoenaed for the taking of a deposition shall designate one or more officers, directors, or managing agents, or other persons who consent to testify on its behalf, and may set forth, for each person designated, the matters on which the person will testify. Federal Rules of Civil Procedure, 30(b)(6).

ISSUING OFFICER'S NAME, ADDRESS AND PHONE NUMBER <i>James R. Starr, Clerk</i> United States District Court for the District of New Hampshire	DATE 9/30/99
--	-----------------

<sup>1</sup> (See Rule 45, Federal Rules of Civil Procedure, Parts C & D on Reverse)

If action is pending in district other than district of issuance, state district under case number.

UNITED STATES DISTRICT COURT  
DISTRICT OF NEW HAMPSHIRE

\*\*\*\*\*  
In re: WPI Group, Inc. \*  
\* CIVIL ACTION No. Misc-99-\_\_  
\*\*\*\*\*

**REQUEST FOR ISSUANCE OF SUBPOENA  
TO SERVICE PROVIDER  
PURSUANT TO 17 U.S.C. § 512(h)**

NOW COMES WPI Group, Inc., by and through its counsel, McLane, Graf, Raulerson & Middleton, Professional Association, and requests that this Court issue a subpoena to a service provider for identification of an alleged copyright infringer, pursuant to 17 U.S.C. § 512(h). In support of this request, WPI Group, Inc. states as follows:

**PARTY AND JURISDICTION**

1. Requestor, WPI Group, Inc. is a New Hampshire corporation, with its principal place of business at [REDACTED]. Its world wide web address is: [REDACTED]

2. This court has subject matter jurisdiction over this matter pursuant to 17 U.S.C. § 512(h) as well as 28 U.S.C. § 1338(a).

**BASIS FOR REQUEST**

3. On August 18, 1999, WPI Group, Inc. discovered that a web page existed on the internet containing libelous information about WPI Group, Inc. and its chief executive officer. That web page included a copy of a photograph of WPI Group, Inc.'s chief executive officer. That photograph is a duplicate of the photograph appearing in WPI Group, Inc.'s 1998 annual report. WPI is the owner of the copyright to that

photograph, and has legal rights in it, even though it has not yet sought copyright registration. See, 17 U.S.C. §§ 102, 408. See also, Arthur Rutenburg Homes, Inc. v. Drew Homes, Inc., 28 F.3d 1529 (5<sup>th</sup> Cir. 1994). WPI Group, Inc. never licensed its copyright of that photograph to any other party.

4. That unauthorized copy of the photograph of WPI Group, Inc.'s chief executive officer appeared on a web page with the domain name "wpigroup.homepage.com." The second level and top level domain address, "homepage.com," is registered to HomePage.com, Inc.

5. HomePage.com, Inc. is a corporation located at 130 West Union Street, Pasadena, California. It is in the business of providing online services to customers, by which a customer may post its own web page from HomePage.com, Inc.'s computer server. Building upon HomePage.com, Inc.'s domain name, a customer may choose its own third level domain name to be used in conjunction with the HomePage.com, Inc. second and top level domain names. As such, HomePage.com, Inc. is a service provider as defined in 17 U.S.C. § 512(k)(1) and may be subpoenaed pursuant to 17 U.S.C. § 512(h).

#### **REQUEST FOR RELIEF**

6. WPI Group, Inc. requests the issuance of a subpoena to the service provider, HomePage.com, Inc. so as to identify its customer who is an alleged infringer of WPI Group, Inc.'s copyright.

7. Such a request is justified pursuant to 17 U.S.C. § 512(h). As required by 17 U.S.C. § 512(h)(2), attached to this request is (a) a copy of notification to

HomePage.com, Inc. in accordance with 17 U.S.C. § 512(c)(3)(A); (b) a proposed subpoena; and (c) a sworn declaration.

8. HomePage.com, Inc.'s counsel has confirmed to counsel for WPI Group, Inc. that it has already received notification substantially complying with 17 U.S.C. § 512(c)(3)(A) and will cooperate with WPI Group, Inc. in producing information should a subpoena be issued. HomePage.com, Inc. will not, absent a subpoena, turn over this information to WPI Group, Inc.

9. WPI Group, Inc.'s counsel has prepared a subpoena according to Federal Rule of Civil Procedure 45, which is incorporated to the extent possible in this request, pursuant to 17 U.S.C. § 512(h)(6).

WHEREFORE, WPI Group, Inc. requests that this Court issue a subpoena to HomePage.com, Inc. in the form attached hereto as soon as possible.

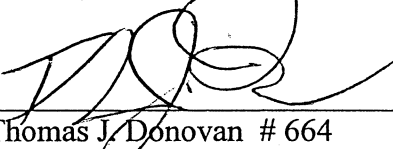
Respectfully submitted,

WPI GROUP, INC.  
By Its Attorneys,

McLANE, GRAF, RAULERSON &  
MIDDLETON, PROFESSIONAL ASSOCIATION

Dated: September 29, 1999

By: \_\_\_\_\_

  
Thomas J. Donovan # 664  
900 Elm Street, P.O. Box 326  
Manchester, NH 03105-0326  
Telephone: (603) 625-6464

57976



McLane, Graf,  
Raulerson &  
Middleton

Professional Association

NINE HUNDRED ELM STREET • P.O. BOX 326 • MANCHESTER, NH 03105-0326  
TELEPHONE (603) 625-6464 • FACSIMILE (603) 625-5650

THOMAS J. DONOVAN  
(603) 628-1337  
tdonovan@mclane.com

OFFICES IN:  
MANCHESTER  
CONCORD  
PORTSMOUTH  
NASHUA

September 28, 1999

Via Facsimile:310-312-3786  
and U.S. First Class Mail

c/o George M. Borkowski  
Ms. Debby Porter  
HomePage.com, Inc.  
130 West Union Street  
Pasadena, CA 91103

Re: WPI Group, Inc. v. HomePage.com, Inc.  
99-E-0358

Dear Mr. Borkowski:

This letter follows up on my letter dated August 19, 1999 notifying HomePage.com, Inc. of the unauthorized publication of material on the wpigroup.homepage.com website. Let me confirm that at least a portion of the offensive material that appeared on that website, the photograph of the chief executive officer of WPI Group, Inc., is a copyrighted work, and its publication was not authorized by WPI Group, Inc., the copyright owner. This notification, as was the prior notification, is submitted under penalty of perjury and is intended as a notification pursuant to 17 U.S.C. § 512(h)(3)(A).

Very truly yours,

  
Thomas J. Donovan

TJD

cc: Michael B. Tule, Esq.  
59796



McLane, Graf,  
Raulerson &  
Middleton

Professional Association

NINE HUNDRED ELM STREET • P.O. BOX 326 • MANCHESTER, NH 03105-0326  
TELEPHONE (603) 625-6464 • FACSIMILE (603) 625-5650

THOMAS J. DONOVAN  
(603) 628-1337  
tdonovan@mcLane.com

OFFICES IN:  
MANCHESTER  
CONCORD  
PORTSMOUTH  
NASHUA

August 19, 1999

Via Facsimile: 626-535-2701  
and U.S. First Class Mail

Copyright Agent  
HomePage.com, Inc.  
130 West Union Street  
Pasadena, CA 91103

Re: [www.wpigroup.homepage.com](http://www.wpigroup.homepage.com)

Dear Copyright Agent:

This firm represents WPI Group, Inc., a publicly traded New Hampshire corporation listed on NASDAQ. It is an international technology-based company with subsidiaries in various locations in the United States and abroad. Its chairman and chief executive officer is [REDACTED]. WPI's domain name is [www.wpigroup.com](http://www.wpigroup.com).

My client was shocked to discover yesterday that HomePage.com, Inc. has registered the second level domain name "wpigroup" to someone not authorized by WPI Group, Inc. and directly in violation of WPI Group, Inc.'s property rights. It also creates the metatag "WPI Group," which will attract search engine "hits" from inquiries about WPI Group, Inc. Moreover, the content of HomePage.com, Inc.'s web page, [wpigroup.homepage.com](http://wpigroup.homepage.com), contains the unauthorized photograph of WPI Group, Inc.'s chairman and chief executive officer, as well as statements libelous to him and to WPI Group, Inc.

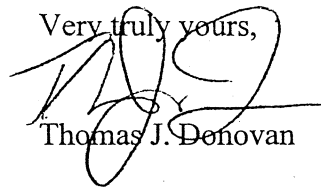
I have reviewed the terms of service under which HomePage.com, Inc. offers its members the opportunity to post web pages using HomePage.com, Inc.'s server. Those terms of service prohibit posting on member web pages, among other things, libelous material, impersonation of an entity, violation of state or federal laws, and infringement of the proprietary rights of any party. The terms of service also purport to absolve HomePage.com, Inc. from responsibility for the content of these web pages. That language may attempt to protect HomePage.com, Inc. from liability for the internal content of a web page, but it certainly can not

protect HomePage.com, Inc. from registering a web page name which violates the property rights of an entity, such as WPI Group, Inc.

This letter demands that HomePage.com, Inc. cease and desist from registration and publication of both the web page name, wpigroup.homepage.com and any related metatag, as well as from continued publication of the deceptive and libelous statements contained on that web page. I will monitor the website for the next 24 hours. If this offensive material and the unauthorized use of the WPI Group, Inc. name is not removed by that time, my clients have authorized me to seek a temporary restraining order to stop this behavior. This web page violates a number of state and federal statutes, including the Lanham Act and New Hampshire's unfair business practices statute. If this material is not removed, WPI Group, Inc. will also seek money damages against HomePage.com, Inc. WPI Group, Inc. also demands that you provide the correct name and address of any persons responsible for registering the name wpigroup or posting the libelous information on that web page.

I look forward to your response today.

Very truly yours,



Thomas J. Donovan

TJD

cc: Michael B. Tule, Esq.

50828



# CyberSmears & CyberAttacks, Protecting Your Company

ACCA Annual Meeting  
October 2003

Thomas Donovan, partner, McLane, Graf, Raulerson & Middleton  
Hemanshu Nigam, Corporate Attorney, Microsoft  
Bradford Weller, General Counsel, Captiva Software Corporation

## What is a CyberSmear?

- A posting in a public internet forum, such as a bulletin board (Yahoo Message Boards) or a special purpose web site (yourcompanysucks.com)
- Made by an anonymous malefactor
- Which purports to disclose information about a business or its management that is false, defamatory or otherwise potentially actionable
- Distinguished from "CyberGripes," (plain old negative opinions), and from "CyberSquatters", (trademark misuse in URLs, addressed by Anti-cybersquatting Protection Act

## What is a CyberAttack?

- An electronic attack on a website that affects the confidentiality, integrity, or availability of data
  - (Distributed) Denial of Service (DDoS, DoS)
  - Syn Flood Attack
  - Hack
- Consider these responses
  - Technical responses – stop, divert, don't hack back
  - Legal response - Computer Fraud and Abuse Act
    - 18 USC 1030 – Civil or Criminal
  - Policy response – Section 217 of the PATRIOT Act
    - Inviting Law Enforcement onto your premises during attack

## The Role of In-house Counsel

- Management
  - Wants someone to identify and stop the posters.
  - Is emotionally willing to spend “unlimited” resources
  - Doesn't know that what it wants may be illegal or exposes the Company to significant penalties

## Role of In-house Counsel (cont.)

- Preventive Measures
  - Register or acquire web site names that could be misused (i.e. "yourcompanysucks.com" names)
  - Monitor the boards and sites to be as pro-active as possible (this service can be outsourced; see, e.g. markmonitor.com and mediasentry.com)
  - Require nondisparagement and confidentiality provisions in employee/contractor agreements.

## Role of In-house Counsel (cont.)

- Identifying the Issues
  - Is company confidential information involved?
  - Is the company/brand being harmed?
  - Is employee confidentiality violated?
  - Is there any indication that the poster is an employee, ex-employee or a competitor?
  - Will taking action escalate out of control, causing more problems?

## Role of In-house Counsel (cont.)

### ■ The Alternatives

#### ■ Do Nothing

- 1<sup>st</sup> Amendment rights of the poster broadly respected
  - Courts are willing to protect anonymity against subpoenas
  - Interest in public discourse outweighs harm of false statements
  - "No one believes it anyway," or "It's all just opinion." (Global Telemedia)
- 1<sup>st</sup> Amendment rights of companies limited
  - Companies in California have been sued for engaging in public debate (*Kasky v. Nike*)
  - Companies have been punished for trying to stifle the public debate (*Hollis-Eden Pharmaceuticals* -- \$107,887)

## Role of In-house Counsel (cont.)

### ■ The Alternatives (cont.)

- Counter with "Corrective" Disclosures?
  - *Kasky v. Nike* – correcting the record as unfair trade practice
  - Securities Fraud Issues
    - Short Sellers post negative statements to drive stock price down and thus profit
    - Most experienced message board surfers know that obsessive, negative posers are out for own gain
    - Current consensus is that the nature of the forum is so unreliable, so lacking in substance that no one really pays any attention any more
    - Does the SEC care? Sean St. Heart, Release 16947

## Role of In-house Counsel (cont.)

### ■ The Alternatives (cont.)

#### ■ Self Help

- Identify the cybersmearer and contact the person
  - Do it in-house. Use search tools found in Hemanshu Nigam's handout.
    - Decode IP Address and obtain telephone number
    - Whols and other lookup tools
  - Private investigators – beware of hackers
    - Must know how to maintain chain of evidence
    - Must know limits of Electronic Communications Privacy Act/ Stored Communications Act. (see, Theofel v. Farey-Jones)
- Contact bulletin board host and request removal of scandalous, infringing or confidential matter

## Role of In-house Counsel (cont.)

### ■ The Alternatives (cont.)

- Use the judicial system to seek a remedy
  - To make it stop – injunctive relief
  - To identify, expose and punish the poster – bringing a claim for damages
  - It is easier to start a lawsuit than to stop one
  - Can lead to counter suit, govt. investigation (ITEX) and bad publicity (Varian)

## Role of Outside Counsel

- Evaluating Possible Causes of Action
  - Libel
    - Problem of opinion, public figure defense
  - Unfair Trade Practices – Business Disparagement
    - Lanham Act §43(a)
  - Securities Fraud
    - Rule 10(b)(5)
  - Copyright Infringement
    - Unauthorized copies of company documents
  - Trademark Infringement
    - Use okay if not in connection with sale of goods

## Role of Outside Counsel

- Evaluating Possible Causes of Action (cont)
  - Misappropriation of Trade Secrets
    - Must fit within statutory definition
  - Breach of Contract
    - Employment/contractor agreements
  - Property Torts
    - Conversion of domain names or a company's cyberspace
  - ISP Terms of Service
    - Basis for removal of material from site

## Role of Outside Counsel (cont.)

### ■ Fighting Anonymity

- John Doe actions coupled with ex parte subpoena to web host
- Discovery action against web host directly, despite Communications Decency Act
- Digital Millennium Copyright Act (DMCA) subpoenas
- Post the subpoena request on web site?

## Role of Outside Counsel (cont.)

### ■ Procedural & Other Roadblocks

- ISPs Not Liable Pursuant to Sec. 230(c)(1) of the Communications Decency Act
- 1<sup>st</sup> Amendment-inspired prerequisites before obtaining subpoena ([Seescandy.com](http://Seescandy.com); [Dendrite](http://Dendrite))
- Court rule prerequisites to ex parte subpoenas (CCP §2025(b)(2))
- The ISPs may fight back (Verizon)

## Role of Outside Counsel (cont.)

- Procedural & Other Roadblocks
  - Anti-SLAPP Statutes
    - Strategic Lawsuit Against Public Participation
    - Must be “in connection with public issue”
    - If so, plaintiff must prove its prima facie case to avoid special motion to strike



**Cyber-Smeared & Cyber-Attacks:  
Protecting Your Company  
*Basic Online Investigation  
Techniques***

**Hemanshu Nigam  
Corporate Attorney  
Law and Corporate Affairs  
Microsoft Corporation**

**ACCA's 2003 Annual Meeting: Charting A New Course  
October 9, 2003**

**IP Addressing  
Explained**

## Understanding IP Addressing

- IP addresses are a set of numbers assigned to a user or website, usually in the form of a dotted quad:  
Microsoft.com  
IP Addresses:  
  
207.46.249.190, 207.46.249.222, 207.46.249.27,  
207.46.134.155  
207.46.134.190, 207.46.134.222
- Everyone on the Internet has an IP address assigned to them when using the Internet
- Think of IP addresses as your home address, as a location must be established for receiving mail and info, thus in this analogy email and data

## Tools to aid in your investigation

- NSLOOKUP or Name Server lookup is a very handy tool used in determining the IP address of a domain name.
- One of Microsoft.com's multiple IP address is 207.46.249.190.
- Web sites can have more than one IP address allocated to them based on traffic demands.
- Domain names exist because humans have a hard time remembering more than 7 digits.

## **Tools to aid in your investigation**

- **Reverse Nslookup:** Reverse Nslookup is often used to reveal the identity of a domain name of an IP address in question
  - **Doesn't always work as most websites that conduct illegal activities utilize an IP address as the sole URL and while not having a domain name associated with it.**  
**Ex: http://10.10.10.1**
- **Traceroute:** Traceroute is used to verify what part of the country or world a person or server is in.
- **Ping:** The most generic command of your investigation, the ping command is used to verify if an IP address or a website is still alive.

## **Tools to aid in your investigation**

- **WhoIs:** The WhoIs command will tell you who is the registered owner of the site and the ISP that is hosting the site.
  - **Not always accurate**
  - **Information can be falsified rather easily**

## WHOIS accuracy

- ICANN has a uniform policy that WHOIS data must be accurate.
- Once notified, owner of the registered domain must comply with this request to rectify any inaccurate information
- Domain may face deletion from WHOIS database, if not in compliance
- Different registrars have different approaches
- Please see Sec. 3.7.8 for further information:  
<http://www.icann.org/registrars/ra-agreement-17may01.htm>

## RIR WHOIS

- RIR or Regional Internet Registries
- Used to find out the owner/sublessor of an IP block that is assigned to a Website or user
- ARIN – American Registry for Internet Numbers  
[www.arin.net](http://www.arin.net)  
*Region: North America, Africa south of the equator, and portions of the Caribbean*
- APNIC - Asia Pacific Network Information Centre [www.apnic.net](http://www.apnic.net)  
*Region: Asia and Pacific region*

## RIR WHOIS cont'd

- **LACNIC - Latin American and Caribbean Internet Addresses Registry**

[www.lacnic.net](http://www.lacnic.net)

*Region: Latin America and portions of the Caribbean*

- **RIPE – Réseaux IP Européens**

[www.ripe.net](http://www.ripe.net)

*Region: Europe, Parts of Asia, Africa north of the equator, and the Middle East*

## Helpful Free Tools

- **Ping**

<http://www.webmaster-toolkit.com/ping.shtml>

- **Nslookup**

<http://network-tools.com/nslookup/>

- **Reverse NSlookup:**

<http://www.webmaster-toolkit.com/nslookup.shtml>

## Helpful Free Tools

- **Visual Traceroute:**

**<http://www.visualware.com/visualroute/livedemo.html>**

- **WhoIs**

**<http://www.internic.net/whois.html>**