Hospitality Review

Volume 26
Issue 1 *Hospitality Review Volume 26/Issue 1*

Article 6

January 2008

Cybergriping: Violating the Law while E-Complaining

Juline E. Mills
Purdue University, jamills@purdue.edu

Brian J. Tyrrell
Richard Stockton College of New Jersey, null@stockton.edu

William B. Werner
University of Nevada, Las Vegas, null@unlv.nevada.edu

Robert H. Woods
University of Nevada, Las Vegas, null@unlv.nevada.edu

Cybergriping: Violating the Law while E-Complaining

Abstract
The emergence of Web communications has given rise to complaint sites which serve as central forums for both consumers and employees to share their bad experiences. These complaint sites provide for cybergriping in various forms. This paper explores the concept of cybergriping and its relevance to the hospitality and tourism industry from employee and customer perspectives. Court cases in which cybergriping played a key role are reviewed, and recommendations are offered on how hospitality and tourism businesses can address the problem of cybergriping.

Keywords
Cybercrimes, Tourism, Cybergriping

Cybergriping:
Violating the Law While E-Complaining

By Juline E. Mills, Brian J. Tyrrell, William B. Werner, Robert H. Woods and Michael S. Scales

The emergence of Web communications has given rise to complaint sites which serve as central forums for both consumers and employees to share their bad experiences. These complaint sites provide for cybergriping in various forms. This paper explores the concept of cybergriping and its relevance to the hospitality and tourism industry from employee and customer perspectives. Court cases in which cybergriping played a key role are reviewed, and recommendations are offered on how hospitality and tourism businesses can address the problem of cybergriping.

"Hell hath no fury like a hardworking employee or a paying customer scorned" (Wolrich, 2002).

Consider the following hypothetical scenario: You are the manager of Fantastic Resort, an establishment whose management philosophy is based on the WOW effect of delighting both customers and employees (Cohen, 1997). While other resorts at your destination are still suffering from the effects of September 11, 2001, and the subsequent wars in Afghanistan and Iraq, you have a 90% average occupancy. You make a mental note to meet with personnel to discuss re-hiring strategies since you drastically reduced staff in anticipation of the fallout from the wars. In preparation for your vacation, sponsored by your employer, you check your e-mail and see two urgent messages. The first message is from a former disgruntled employee sent to all current employees for the tenth time warning them of the dangers of working for your company. This employee has set up a Web site, www.dontworkforfantasticresort.com, and is encouraging current employees to visit and post their gripes about your company. The second e-mail is from a customer who has registered dissatisfaction with your services at planetfeedback.com, as well as on his recently developed Web sites fantasticresortsucks.com, fantasticresortarecrooks.com, and fantasticresortripoffs.com. As you ponder the e-mails, the managing director, who got the same e-mail, calls, demanding that you fix the problem ASAP and find out how this could have happened. What would you do?

The ease of publishing on the Web has given employees and customers a means of posting their complaints called *cybergriping*. Online complaint forums have global reach and are now readily accessible, unlike traditional print media, television, or radio (Beetlestone, 2002). This article explores the concept of cybergriping and its relevance to hospitality and tourism from the employees' and customers' perspectives. We review court cases in which cybergriping played a key role and offer recommendations on how hospitality and tourism businesses can address the problem of cybergriping.

CYBERGRIPING BACKGROUND

The preferred venue for word-of-mouth communication these days is likely to be the Web rather than the water cooler. Dissatisfied employees and customers are now turning to the Web to file or cybergripe their complaints. The term *cybergriping*, also referred to as *electronic complaining or e-complaining*, is an Internet buzzword associated with Web sites criticizing corporations, organizations, individuals, or products and services (Band & Schruers, 2003). Cybergriping occurs when "one party, the 'cybergriper,' establishes a 'complaint Website' or an 'attack site' dedicated to the publication of complaints, claims, criticism, or parody of or against another party often referred to as the 'target company.' Typically the cybergriper registers the Website under a domain name comprised of the target's trademark and such pejorative suffixes as 'sucks.com,' 'crooks.com,' or 'ripoff.com'" (Newman, 2003). The target company's trademark is included in the attack site's domain name to increase the likelihood that potential customers will retrieve the complaint site each time they attempt to locate the target company's official Web

site or search the Internet for information about the target company. Cybergriping or e-complaining activities may seem harmless at first; however, with approximately 550 million Web searches being conducted daily, via an audience worth two billion dollars a year to online advertisers, a company has a lot at stake and may lose substantial business when a potential consumer stumbles on a cybergriper's Web site that denigrates a company (Grossman, 2003; Benderoff & Hughlett, 2006).

Cypergriping also occurs on third-party sites, where the employee or customer registers a complaint about a company using the services provided specifically for complaining. Examples include Plantfeedback.com, the Better Business Bureau at www.bbb.org, and Complaindomain.com. Some complaint Web sites may also take an active role on behalf of the consumer by trying to contact the business by e-mail or postal mail. Some complaint sites aggregate consumer complaints in an effort to get a particular company to respond to a persistent product or customer service problem (Ponte, 2001). Online complaint services primarily provide employees and consumers with an opportunity to vent their dilemma typically through chat rooms or message boards (forums). Planetfeedback.com, in addition to providing a forum that allows participants to identify a company by name and industry, also provides a list of companies that respond quickly and efficiently to customer comments. These companies include Krispy Kreme Doughnut Corporation and Chick-Fil-A Inc., which are described as quick responders to customer complaints; and Ramada Franchise Systems Inc. and Budget Rent-A-Car System Inc., which are described as among the worst in dealing with consumer complaints (Jackson, 2003). Other notable third party complaint sites include EComplaints.com (one of the first but now defunct), as well as TheComplaintStation.com, Baddealings.com, FightBack.com, Complaint.com, and Ripoffreport.com (also defunct). Popular employee complaint sites include VaultReports.com Electronic WaterCooler(TM), the first-ever network of more than 1000 company-specific bulletin boards; FACE Intel, a site for former and current employees of Intel; Disgruntled.com, where more than 30,000 employees vent workplace frustrations monthly; and www.xmci.com, "dedicated to everyone from MCI who has been downsized, rightsized, outplaced or even headhunted out" (Moebius, 1999). The federal Occupational Safety & Health Administration (OSHA) has also set up a Web site to hear employee complaints.

The term *cybergriping*, rooted in the complaint behavior literature, means "to express grief, pain, or discontent" or "to make a formal accusation or charge" regarding "something that is the cause or subject of protest or outcry (complaint)." Employee satisfaction research contends that two out of ten unsatisfied employees stay less than two years with a company, and that dissatisfied employees are not likely to recommend their company to a friend, potentially making it more difficult for a company to recruit future top-quality employees or attract and retain customers (Business Research Lab, 2004). In 2002 a survey of 2,200 hourly and salaried workers by CareerBuilders.com reported that 38% of the respondents were dissatisfied with their current positions and were job hunting. Half of those planning to change jobs said they worked under a great deal of stress, while others cited poor prospects for career advancement, lack of job security, and low pay as aggravating circumstances (LaMonica, 2002). This situation worsened in 2003, when a survey of 2,400 full- and part-time workers at companies with 50 or more employees revealed that only 30 % of employees were loyal and committed to staying with their company over the next two years. Employee turnover can cost large companies millions in recruitment and training, and replacing professional employees can cost as much as 18 months' salary (Southerland, 2003). Disgruntled employees can spread their dissatisfaction and sinking attitude to other employees, thereby severely affecting an entire organization's productivity. An angry employee may even seek retaliation by destroying property or attempting sabotage. A lack of employee commitment to job performance may in turn lead to dissatisfied customers.

Customer complaining behavior is "a set of multiple (behavioral and non-behavioral) responses, some or all of which are triggered by perceived dissatisfaction with a purchase

episode" (Singh, 1988). Singh developed a typology of customer-complaint responses, classifying complaining behavior as either third party (complaints lodged with some independent organization), voice (complaints lodged with the faltering company), or private (complaints lodged with family or friends). In 1981, research studies by Technical Assistance Research Programs (TARP) revealed that dissatisfied customers engage in twice as much word of mouth as satisfied customers. These findings were supported by research that showed dissatisfied customers use word of mouth to tell their stories from two to ten times as often as satisfied customers (Schlossberg, 1990). Love (2001) reported that happy customers tell from five to six people, while unhappy customers tell from eight to ten, and 10% of unhappy people tell 20 or more other people. How the Internet has affected these statistics has yet to be quantified, although buzzwords like *viral marketing, peer marketing, chatter,* and *online posting* attest to the fact that the Internet is well utilized as a medium for customers to vent their frustrations to a larger audience—especially when customers believe that management does care about them (Snyder, 2004). Known as the "tip of the iceberg phenomenon," about 45% of customers in all industries will complain about a problem to a front-line person. Chances are high that the problem will never be reported to the manufacturer or to the corporate office. Further, only about 1% to 5% of customers will escalate their complaint to a local manager or corporate headquarters. In a survey of airlines, TARP also found that only 3% of consumers unhappy about their airline meal complained to anyone, and then only to flight attendants. No complaints were made to the corporate headquarters or to consumer affairs (Goodman, 2004).

The "butterfly customer" and the "customer has escaped" philosophies provide some explanation for the increasing usage of cybergriping by consumers. O'Dell and Pajunen (1997) proposed the "butterfly customer" concept, referring to consumers who have been transformed from loyal, reliable, and predictable patrons into transients—here today, flitting across the street tomorrow. The butterfly customer is constantly in motion for the best deal, the best choice, and the latest trend. This "creature" selects a store or brand at random, often abandoning the tried and true for the newest, the closest, and the cheapest. Nunes and Cespedes (2003), in an article aptly titled "The Customer Has Escaped," describes today's customers as channel surfers who shop for information from one channel, then defect from that channel when it comes time to purchase the item. With the advent of the Internet, consumers are freed from time and place constraints, and are allowed to quickly and easily carry out repeated transactions. Consumers demanding quicker services have gravitated towards companies that provide the closest to instantaneous delivery. Consumers actively choose whether or not to access a company's information both on and offline and are exercising unprecedented control over the management of the content with which they interact (Abramson & Hollingswood, 2004). The growth in Weblogs, personal journal entries which in many cases are personal accounts of people who want to share some aspect of their lives with others (Douglas & Mills, 2006), has increased the scope and reach of cybergriping. Reports that detail the top corporate hate sites indicate this reach (Wolrich, 2005). The hospitality and tourism industry is no stranger to e-complaining. In one of the industry's earliest incidents, a Connecticut man in 1998 built a complaint site, now defunct, against Dunkin Donuts Inc. (dunkindonuts.org), because the chain did not carry his favorite low-fat coffee creamer. Other customers could also post complaints against the company at this site. Dunkin Donuts Inc. learned this could be valuable and used the Web site to apologize to complaining customers and offer them compensation. The Web site became so popular that Dunkin Donuts Inc. eventually bought the site for an undisclosed sum of money (Hearn, 2000). Indicating the need for the hospitality and tourism industry to address the growth of cybergriping are statistics revealing that more than 700 firms subscribe to a service called eWatch.com, which monitors Usenet groups, online service forums, and Web bulletin boards for comments related to companies (Baldwin, 1999; PR Newswire, 2006). However, the companies that have been targets at cybergripe sites respond to less than 1% of the complaints (Appelman, 2001). Airline sites such as Continental, Delta, Northwest, and United have addressed consumer

complaints by providing e-mail addresses on their Web sites. However, other airlines, such as Southwest, do not accept e-mails due to time demands, but they do accept complaints by telephone and mail. Not all complaint site stories are successful for hospitality and tourism firms. Table 1 presents a global overview of some hospitality and tourism cybergripe sites started by consumers, and the rationales behind the formation of the Web sites.

Table 1

Hospitality and Tourism Cybergripe Sites

Web Site URL(Address)	Target Company/ Industry	Rationale for Website Formation
www.ctyme.com/circus/	Circus Circus Hotel/ Hotel/Casino	Concerned about a hotel surcharge, this guest complained and felt his complaint was not properly addressed.
www.untied.com/	United Airlines/ Airline	After a lack of timely and appropriate responses to complaints via traditional mail, a business man setup the Web site to voice complaints against United Airlines.
www.brescom.clara.net/ British_Airways.htm	British Airways/ Airline	This traveler is concerned about safety at British Airways.
www.virginaircrewlies.com/	Virgin Airlines/ Airline	This customer had an altercation with a flight attendant that led to his arrest and feels the facts of the case were not presented accurately by the airline or its crew.
www.ncl-sucks.com/	Norwegian Cruise Lines/ Cruise Line	A cruise was diverted several times and this patron felt that no one at the company was willing to compensate for the changes.
www.alitaliasucks.com/	Alitalia/ Airline	Having lost his luggage on a recent trip, the consumer complained to Alitalia and was promised compensation. Not having received adequate compensation, the consumer then began the Web site.
www.northwestsucks.com/ and www.northworstair.org/	Northwest Airlines/ Airline	Formed by a traveler who experienced poor service on more than one occasion.
boycottdelta.org/	Delta Airlines/ Airline	This political activist is concerned about Delta Airlines' cooperation with the Department of Homeland Security's Computer Assisted Passenger Prescreening System (CAPPS II). They feel their Fourth Amendment rights are being violated by CAPPS II.
www.dontspyon.us/	Galileo/ Travel	Created by the same individuals and for similar reasons as boycottdelta.org, this Web site is concerned about Galileo's involvement with CAPPS II.
www.dubaitourism.co.ae/www/eservices/ecomp.asp	(DTCM)/ Tourism	This government operated Web site seeks to solicit complaints about Dubai or Dubai-based establishments from the traveling public.
www.mcspotlight.org/	McDonald's Restaurant	The creators of this site are concerned about McDonalds and other transnational companies.
www.ihatestarbucks.com/	Starbucks/ Restaurant	This individual is concerned about current wages, growth strategies, and ecological practices of Starbucks.
www.themeparkcritic.com	Non-specific/ Amusement Park	The creators wanted a place where theme park visitors could voice their own opinion about theme parks.
www.nconnect.com/%7Emikevb/thrifty.htm	Thrifty Car Rental Car Rental	The Web site owner's car was hit by an uninsured driver who had rented a car from Thrifty Car Rental and was not compensated.

LEGAL THEORIES APPLICABLE TO CYBERGRIPING

Some target companies have attempted to combat cybergriping by bringing suit against cybergripers, citing trademark infringement and dilution, and trade dress violations as grounds. A review of applicable legal theories, however, revealed few reliable means of relief.

Trademark Infringement

When cybergriping, the e-complainers typically include a derivative of the company's trademark with which they have a gripe. A trademark is defined under the Lanham Act of 1976 as "a word, name, symbol, or device or any combination thereof including a sound, used by any person to identify and distinguish goods from those of others." The Lanham Act was created both to protect businesses from unfair competition and to establish a civil cause of action for the deceptive and misleading use of trademarks. Generally, trademarks are classified into four categories: (1) generic, (2) descriptive, (3) suggestive, and (4) arbitrary or fanciful. A generic trademark represents the good or service itself, such as a picture of a generic airplane, hotel room, or food item, and may never acquire trademark protection. A descriptive trademark conveys a "direct indication of the ingredients, qualities or characteristics of the goods" but does not identify the source of those goods. An advertisement containing a picture of a Big Mac sandwich without identifying it as a McDonald's product is an example. A descriptive trademark receives trademark protection only if it acquires a "secondary meaning," which identifies the source of the goods. In contrast, suggestive and arbitrary or fanciful trademarks are inherently distinctive, and thus receive full protection immediately upon their use. A suggestive trademark requires "imagination, thought and perception to reach a conclusion as to the nature of the goods" (Lanham Act 1998). For example, the slogan "Have it your way," by Burger King Brands, Inc., is a suggestive trademark. A trademark is arbitrary or fanciful if it "has no inherent relationship to the product or service with which it is associated," such as "Amazon.com."

A trademark's qualification for protection as one of the above types, however, does not guarantee a remedy for any other use of it. A successful trademark infringement claim requires proof of two elements: (1) prior rights to the protected trademark and (2) the likelihood that unauthorized use of the trademark will cause consumer confusion, deception, or mistake. This second factor, known as the *likelihood of confusion* test, is the touchstone of trademark infringement as a means of seeking legal recourse against cybergripers. Although the standard to determine likelihood of confusion varies among the federal circuits, a typical balancing test will incorporate these eight factors: (1) the similarity of the marks, (2) the proximity of the goods, (3) the marketing channels used, (4) the defendant's intent in selecting the mark, (5) the type of goods and the degree of care likely to be exercised by the purchaser, (6) the evidence of actual confusion, (7) the strength of the mark, and (8) the likelihood of expansion of the product lines (Ferrera, Lichtenstein, Reder, August, & Schiano, 2000).

Trademark Dilution

Businesses may seek recourse against cybergripers through the 1995 Federal Trademark Dilution Act (FTDA), which has expanded the scope of rights granted to famous and distinctive trademarks under the Lanham Act. Dilution differs from normal trademark infringement in that there is no need to prove a likelihood of confusion to protect a trademark from dilution. Instead, all that is required is proof that the use of a "famous" mark by a third party causes the dilution of the "distinctive quality" of the mark. The courts defined *dilution* as "the gradual whittling away of a distinctive trademark or trade name." The FTDA generally recognizes two distinct types of dilution -- *blurring* and *tarnishment*. Blurring occurs when an individual uses or modifies the mark of another entity to identify goods that are different from the plaintiff's, but in such a way that the mark may no longer be fully associated with the plaintiff's product. In contrast, tarnishment occurs when the individual's use of someone's mark degrades the quality of the mark or creates a negative association with it. Under the FTDA, the owner of a famous

trademark that is diluted is entitled to a nationwide injunction. However, if the owner establishes that an individual willfully intended to trade upon the reputation or goodwill of the famous mark, the owner is also entitled to traditional trademark infringement remedies. These remedies include disgorgement of the individual's profits and direct damages sustained by the plaintiff. Many commentators believe that the FTDA is the strongest weapon against the unauthorized use of a trademark and one of the best recourse measures against cybergripers. In one dilution case, *Hasbro Inc. v. Internet Entertainment Group, Inc. (1996)*, involving unauthorized use of a domain name, the toymaker Hasbro successfully sued the owner of a pornographic Web site "candyland.com," on the basis that the use tarnished the trademark-protected game "Candy Land." Though the FTDA may be the strongest weapon against domain-name dilution and similar cases, its broad language is troublesome. Specifically, courts are split on these questions:

(1) What qualifies as a "famous mark" under the statute? What is entitled to protection against dilution of its distinctive nature? What is necessary to prove dilution? (Ramirez, 2001; Lockwood & Nixon, 2005).

Trade Dress Violations

Cybergripers may set up complaint Web sites that are similar in look and feel to the company Web site with which they have a gripe. When two sites have the same appearance, though the content presented may be different, the result causes consumer dissatisfaction. This is particularly challenging when one considers that the Web site may be a company's primary means of communicating with consumers. Landing at a cybergripe site that is disturbingly similar to a company Web site may cause the consumer to distrust and refuse to do business with an organization. This raises a question: What protection is available to the overall appearance of a Web site? The answer to this question lies in *trade dress* law: "Trade dress is broadly defined as the total image and overall appearance of a product or service and may include features such as size, shape, color or color combinations, texture, graphics, or even particular sales techniques. A trade dress is entitled to protection under the Lanham Act if it is inherently distinctive or has acquired secondary meaning. Unlike trademarks, trade dress that is either inherently distinctive or has acquired distinctiveness does not enjoy protection under the Lanham Act unless such trade dress is also non-functional" (Xuan-Thao, 2000; Lanham Act, 1998). However, it must be noted that proof of secondary meaning is not necessarily required in trade dress infringement cases. In *Two Pesos, Inc. vs. Taco Cabana, Inc. (1992)*, two fast-food Mexican restaurants faced off over similar restaurant design and décor. The U.S. Supreme Court held that inherently distinctive trade dress is held protectable from infringement under federal trademark law without proof of secondary meaning. Thus, in order to claim trade dress violation or infringement against a cybergriper, a Web site must prove that the Web site has inherent distinctiveness, secondary meaning, and functionality. One approach to ensuring trade dress protection of the overall look and feel of a company's Web site is to update the data present on the Web site without changing the layout and organization (Xuan-Thao, 2000). However, while this makes sense, trade dress protection is challenged by the basic principle of WYSIWYG (what you see is what you get), as the Web site may display differently from computer to computer based on the type of computer being used, screen resolution, browser, and modem speed (Kellner, 1994).

Cyberchattel

While existing legal rights are satisfactory for some electronic violations, others are addressed by federal legislation, such as anti-hacking, copyright and trademark protections, and by state criminal and defamation laws. However, none of the current federal or state laws explicitly prohibits a disgruntled employee from accessing a business's Web site or Intranet for a purpose that is adverse to the business, such as publishing unflattering or scandalous information. Businesses that have resorted to civil litigation have relied upon common law and

tort law of trespass (trespass to chattel), but have found that its application to Internet communications is not certain or reliable.

For centuries, common law has recognized the concept of a trespass to chattel. A *chattel* generally is tangible personal property, such as a car or computer hardware. When a chattel is damaged or destroyed, the liability to the owner is determined by calculating the amount of the financial loss caused by the trespass. Even when no physical or permanent damage is done to the chattel, the law generally allows an action against the trespasser to compensate the owner for having been deprived possession of the chattel for the duration of the trespass (Prosser & Keeton, 1984). For most types of personal property it is not possible for two parties to have possession of the property simultaneously; hence, an injunction is necessary to reinstate the owner's possession of the property. The case of unauthorized access to computer systems, however, does not always impair the owner's possession or use of the computer hardware or software at the same time. For this reason, when the chattel in question is cyberchattel, the laws of trespass are not easily applied. In one of the first cases confronting cyberchattel, *eBay, Inc. v. Bidder's Edge, Inc. (2000)*, a federal district court in California granted an injunction against unauthorized computer data access on the basis that the trespass into the system in theory deprived the owner of the ability to use the same data bits simultaneously. EBay won the injunction against Bidder's Edge, which used an automated querying program to obtain information off the eBay Website for its own commercial use. EBay claimed that the computer hardware is its property; therefore, it maintains the right to exclude others from using or possessing its hardware. The court's acceptance of this theory seemed to provide a potentially powerful weapon against a variety of unwanted Internet communications and access. Likewise, in *Intel Corp. v. Hamidi (2003)*, the plaintiff won an early victory in legal proceedings to enjoin a former employee from flooding the company's Intranet with unwanted e-mails. The state trial court concluded that the act was a common law trespass and that the harm caused to Intel was sufficient to support an injunction against further unwanted e-mails. In June 2003, however, the California Supreme Court reversed the injunction and held that while in the smallest technical sense Hamidi had used Intel's property without Intel's permission, there was no actual harm done to Intel's property rights and thus no trespass to chattel. The court rejected Intel's claim of deprivation on the basis that Hamidi's use of the e-mail system did not and could not have actually deprived Intel of its concurrent use of the same property for authorized and official e-mails. These cases, *eBay, Inc. v. Bidder's Edge, Inc. (2000)* and *Intel Corp. v. Hamidi (2003)*, demonstrate the uncertainty a business will face when attempting to use state trespass laws to stop unwanted cybergriping on its own computer systems.

Jurisdiction is Still a Problem

While businesses may use the above-mentioned theories to seek recourse against cybergripers, the businesses still have to ensure that they are pursuing litigation in the right courts. For example, while MC Spotlight.com was established to attack the business policies and operations of McDonald's Corporation, that corporation's ability to complain or file suit against the company was limited as the Web site was housed on servers in the Netherlands.

Even when a company has a strong legal claim for cybergriping damages based on theories of online infringement or squatting, the question remains which, if any, court has jurisdiction to hear and decide the case (Wilson, 2000). The established law of personal jurisdiction is based primarily upon the physical locality of the parties, which is rarely relevant and sometimes indeterminable in an online setting. For example, in *Oasis Corporation v. Judd (2001)*, the plaintiff's principal place of business was in Columbus, Ohio, where he manufactured and distributed water coolers both nationally and internationally. The defendant, Judd, was a resident of Oklahoma and president of a computer-software design company with its principal place of business in Pryor, Oklahoma. Judd, the defendant, had never been to or conducted business in Ohio. In 1998, a fire burned out the building where Judd had his Oklahoma

business. Judd believed that fire had been caused by an Oasis water cooler, which had been leased to another building tenant. Efforts by Judd to secure compensation for the losses sustained in the fire from their insurer as well as the plaintiff were unsuccessful. Subsequently Judd launched a gripe site at www.boycott-em.com, on which complaints about Oasis, its officers, and its employees were voiced. Judd displayed Oasis-registered trademarks and trade names on the site and made available the e-mail addresses and telephone numbers of the officers and employees of Oasis. The site also contained an automatic letter-generating system, which allowed visitors to dispatch pre-written letters to the media and Oasis with a single click. Judd never offered any goods or services for lease or sale on the site. In 2000, Oasis sued in an Ohio court for damages in excess of 13 million dollars and for injunctive relief to prohibit Judd from using the Web site to comment on the plaintiff's products and actions. Oasis alleged, among other claims, trademark infringement; false designation of origin, descriptions, and representations; and dilution of a famous mark. The plaintiff's claim was dismissed when the court found itself lacking jurisdiction over the defendant because Judd'sWeb site did not specifically target an Ohio audience. In addition, the fact that Judd could foresee that the Web site would be viewed and have an effect in Ohio was not, in itself, enough to establish personal jurisdiction over him in an Ohio court.

Oasis Corporation v. Judd demonstrates an important legal distinction between business-to-business and business-to-consumer litigation of online claims. State and federal courts now generally agree that a person or company doing business online can be sued in any state where its online customers reside or where its online communications or solicitations are sent or accessed. In cases of direct online commerce, such as a hotel accepting reservations online, it is easy to see that about any court in the country would have personal jurisdiction over the business. However, *an e-complaint on a Web site is not commerce and, for legal purposes, exists only where the hardware storing it is located.* The ability of persons outside a state to access the Web site on the Internet does not confer personal jurisdiction over the site to the state's courts. This does not mean a company cannot sue the perpetrator in a legitimate case, say for defamation or infringement, when the suspect resides elsewhere. It does mean that the company will have to sue in the defendant's home state and therefore likely incur additional legal expenses.

EMPLOYEES AND EMPLOYERS IN THE CYBERGRIPING DEBATE

Businesses have five tasks when dealing with cybergriping. These include (1) protecting the business's reputation from cybergriping customers and employees, (2) protecting employees from harassing customers, (3) protecting customers from employees who wish to publicly complain about the company, (4) protecting employees from cybergriping co-workers, and (5) protecting the business, customers, and employees from other businesses cybergriping against them.

Trademark Infringements against Employees

In 1999 over 30,000 employees filed complaints monthly at disgruntled.com before the Web site was shut down (Beyette, 1999). In an attempt to control the damage caused by disgruntled employees, some employers have sued employees for setting up gripe sites with equal rulings. In *ASDA Group Limited v. Kilgour* the defendant's site, asdasucks.net, received a favorable ruling from an administrative panel of the World Intellectual Property Organization (WIPO) (Sinrod, 2002). The WIPO, a Geneva-based United Nations organization, arbitrates intellectual property (IP) disputes. ASDA, the complainant, owns and operates a superstore chain in the United Kingdom, while the respondent, Kilgour, was described by WIPO as a "disgruntled ex-employee." While employed by ASDA, Kilgour registered the domain name asdasucks.net and operated asdasucks.co.uk. The content of asdasucks.net was directed at ASDA corporate management, which the WIPO panel described as "scandalously and disgustingly abusive." ASDA's complaint, called asdasucks.net "confusingly similar" to its

trademark and said the domain name was registered in bad faith and was "inherently likely to lead some people to believe that the complainant is connected with the domain name." The WIPO noted that this was not a solid argument or grounds for finding in ASDA's favor. In ruling in favor of Kilgour, who never bothered to respond to the complaint, aWIPO panelist, commented that "by now, the number of Internet users who do not appreciate the significance of the '-sucks' suffix must be so small as to be 'de minimis' (i.e., smaller than the Austin Powers' 'mini-me' character) and therefore not worthy of consideration." While Kilgour's linking of asdasucks.net to ASDA's official site at asda.co.uk may have amounted to a confusing use of its domain name, the usage did not equate with asdasucks.net's being confusingly similar to ASDA's trademark. The only conceivable confusion regarding asdasucks.net could arise for Web visitors not fluent in English who "do not therefore appreciate the significance of the '-sucks' suffix" (Sinrod, 2002).

Employers Suing Employees for Defamation Actions

Colden (2001) and Goldstein (2003) note that corporations are increasingly pursuing legal action against their online critics. Employers have sued former employees claiming defamation. In *Vail-Ballou Press, Inc. v. Tomasky (1999)* the defendant had been employed by the plaintiff for nearly five years when he was discharged for using foul and abusive language, assaulting and threatening a co-worker, and insubordination. Following his discharge, he picketed outside the plaintiff's place of business; allegedly threatened former co-workers; sent electronic mail to the plaintiff's customers, potential customers, employees, competitors, and the media detailing the events surrounding his termination; and finally developed a Web site accusing the plaintiff of falsifying documents and statements to various federal, state, and local agencies as well as terminating him for exposing this "corruption." The plaintiff commenced action seeking a permanent injunction against defamation, malicious injury, and wrongful interference with its business relations and contracts. The court agreed that the content of the site was defamatory and granted the injunction. In a similar case, *Varian Medical Systems, Inc. v. Delfino (2003)*, two corporations filed suit against two former employees for defamation, invasion of privacy, breach of contract, and conspiracy after the defendants used Internet bulletin boards to post derogatory messages about the plaintiffs. The defendant, Delfino, had been employed as a senior engineer and had been fired based on complaints that he had been disruptive and had harassed both managers and co-workers. Immediately after Delfino was fired, he began a campaign of posting derogatory messages about the plaintiffs on Internet bulletin boards such as Yahoo. A jury found Delfino liable for defamation and determined that he had acted with malice, fraud, or oppression. The jury awarded the plaintiffs more than half a million dollars in both general and punitive damages. In addition, the trial court also issued a permanent injunction to prevent future injury. Hospitality employers would do well to develop cybergriping rules that govern workplace actions on cybergriping and to educate employees. While the employer may have won the case, such lawsuits strain employer-employee relations.

On the other hand, employees have sued employers for defamation by using Internet postings. In one of the earliest cases, *Blakely vs. Continental*, a female pilot sued Continental Airlines for defamatory messages posted on an Internet bulletin board by fellow pilots (Mills, Hu, Beldona, & Clay, 2001). In *Du Charme v. International Brotherhood of Electrical Workers, Local 45 (2003)*, the plaintiff sued the defendants for breach of contract, covenant of good faith and fair dealing, wrongful termination in violation of public policy, and defamation or libel. The essence of this complaint was that the plaintiff had been wrongfully terminated, and a defamatory statement about the plaintiff's termination had been posted on Local 45's Web site. Despite various motions filed by the defendant, the courts allowed the lawsuit to proceed. Hospitality employers are reminded here that caution needs to be taken when revealing information on a Web site about any actions deemed inappropriate by an employee who has been terminated. As the restaurant industry is fraught with stories of unfair work practices against employees, some

Web sites have been set up to voice the work experiences of individuals employed in the restaurant industry. These Web sites include ShamelessRestaurant.com and Stainedapron.com. ShamelessRestaurant.com (2006) sees its role as "providing the public with restaurant reviews from the employee's perspective" as well as to " to provide a forum in which restaurant employees can air their employment grievances and, at the same time, share information with each other about the worst practices of employers." Restaurant industry executives would do well to continually pursue such sites to see what employees are saying about their company and what reasonable actions should be taken to deal with employee online complaints.

Employees Suing Employers (The Griper's Right to Privacy)

Employees may contend that their Web postings are private expressions of free speech that take place outside of work hours. Thus, they are of no concern to the employer. However, the right of a company to know what its employees are saying about it was demonstrated in *Konop v. Hawaiian Airlines, Inc. (2003)*. The plaintiff, a pilot for Hawaiian, created and maintained a Web site where he posted bulletins critical of his employer, its officers, and its union, the Air Line Pilots Association (ALPA). Konop controlled access to his Web site by requiring eligible visitors, mostly pilots and other employees of Hawaiian, to log in with a username and password. Konop programmed the Web site to allow access when a person entered the name of an eligible person, created a password, and clicked the "submit" button on the screen, indicating acceptance of the terms and conditions of use. The terms and conditions prohibited any member of Hawaiian's management from viewing the Web site and prohibited users from sharing and disclosing the Web site's contents. Hawaiian's vice president received permission from one of the eligible members to use that member's access to the plaintiff's Web site. The vice president claimed he was concerned about untruthful allegations that he believed Konop was making on the Web site, and accessed the site over thirty-four times. Konop subsequently received a call from the chairman of ALPA, on behalf of the Hawaiian president, who was upset by Konop's accusations and disparaging statements published on the Web site. Konop subsequently filed suit alleging claims under the federal Wiretap Act, the Stored Communications Act (SCA), the Railway Labor Act, and state tort law, arising from the vice president's viewing and use of Konop's secure Web site. Summary judgment was granted to Hawaiian on all charges. In ruling for the defendant, the court noted that Congress had passed the Electronic Communications Privacy Act (ECPA) in 1999 to afford privacy protection to electronic communications. Title I of the ECPA amended the federal Wiretap Act, which previously had addressed only wire and oral communications, to "address the interception of ... electronic communications." Title II of the ECPA created the SCA, which was designed to "address access to stored wire and electronic communications and transactional records." The ECPA protects electronic communications that are configured to be private, such as e-mail and private electronic bulletin boards, while the SCA addresses the growing problem of unauthorized persons deliberately gaining access to electronic or wire communications that are not intended to be available to the public. While Web sites may be public, many, such as Konop's, are restricted. The nature of the Internet, however, is such that if a user enters the appropriate information (password, Social Security Number, etc.), it is nearly impossible to verify the true identity of that user. We are confronted with such a situation here. Although Konop took certain steps to restrict the access of the vice president and other managers to the Web site, the vice president nevertheless was able to access the Web site by entering the correct information, which was freely provided to him by an individual who was authorized to view the Web site. This case provides support for the right of the employer to access such Web sites even without the author's permission.

Employers Being Sued Over the Actions of their Employees

Employers may be liable for the cybergriping actions of their employees. In one case an employee of an Internet service provider (ISP) registered an e-mail address under the name of a long-time employee of the Office of the Attorney General for the Commonwealth of Kentucky,

where a complaint against the ISP had been lodged by an unsatisfied consumer (*Booker v. GTE Net, 2003*). After registering a false e-mail address, the employee of the ISP, it was claimed, sent the complaining customer an e-mail suggesting that the customer had spread libel about the ISP in the complaint to the Office of the Attorney General. The letter also contained inflammatory language that suggested the client was a "grumpy, horrible man who [needed] to grow up" and told the unsatisfied customer he should "put on [his] pampers and ask for [his] booba OR cancel the service altogether." The employee of the Office of the Attorney General sued the ISP claiming that she was traumatized by the incident and suffered emotional and psychological injuries as a result.

While the actions of the employee clearly were not in the best interest of the employer, the plaintiff lost the case. The courts reasoned that the employer could not be held liable "under the doctrine of respondeat superior unless the intentional wrongs of the agent were calculated to advance the cause of the principal or were appropriate to the normal scope of the operator's employment." That is, the plaintiff need to show wherein the actions of the employee were normal duties performed in the course of his/her job and that these actions were advancing the business. Despite the win for the defendant, hospitality and tourism organizations would do well to ensure that employees not become overzealous in defending the organization, as such adverse publicity could be damaging to the reputation of the business. Restaurants in particular need to pay attention to such Web sites as BitterWaitress.com, on which servers dissatisfied with tips left by customers post the customer's name on the "cheapskate list" provided at the site. Such actions are not only damaging to the restaurant but may be seen as cybersmearing by that customer. Little recourse exists for customers who have been defamed on Web sites such as BitterWaitress.com, which are not considered as content publishers but are viewed more as "pipelines" presenting the opinions of their readers and contributors (Benderoff & Hughlett, 2006).

CYBERGRIPING BY CUSTOMERS

The potential challenges and weaknesses of litigating customers who cybergripe is illustrated in *Bear Stearns Companies, Inc. v. Lavalle (2003)*, and *Taubman Company v. Webfeats et al. (2003)*. In *Bear Stearns v. Lavalle*, the court permitted the cybergriper to operate complaint sites named "EMCMortgageFrauds.com," "EMCMortgageScams.com," "EMCMortgageCriminals.com," "BearStearnsFrauds.com," and "BearStearnsCriminals.com," but prevented him from using "EMCMortgageComplaints.com," "BearStearnsShareholders.com," and "BearStearnsComplaints.com." The court reasoned that while the former sites were clearly critical of and thus distinct from the target companies, the latter names were sufficiently deceptive and similar to the target companies' trade names to create confusion and were thus actionable under the trademark dilution provisions of the Lanham Act. A cybergriper may use a target company's trademark in the complaint site's domain name so long as it incorporates a suffix such as "scams.com," "criminals.com," or "frauds.com." In other words, the Web site suffix must be *sufficiently obnoxious and insulting* to dispel any misconception that the complaint site is either the target company's official Web site or is otherwise sponsored by or affiliated with the target company. Even when a cybergriper maliciously incorporates the target's trademark in the complaint site's domain name with the intent of causing the target company commercial harm, a cybergriper's use of the target's trademark on the attack site is non-commercial in nature and therefore beyond the reach of the Lanham Act's prohibitions against trademark infringement and dilution (Lanham Act, 2003).

In *Taubman Company v. Webfeats et al.*, the federal Sixth Circuit Court of Appeals dissolved a trial court's injunction that had protected the Taubman Company and its trademarked shopping mall "The Shops at Willow Bend" from Webfeats' cybergriping. Upon noticing a shopping mall under construction near his home, the defendant registered the domain name, "shopsatwillowbend.com." The Web site featured information about the mall, with a map and

links to individual Web sites of the tenant stores. The site also contained a prominent disclaimer, indicating that the defendant's site was unofficial, and linked to the plaintiff's official site for the mall, found at the addresses "theshopsatwillowbend.com," and "shopwillowbend.com." The defendants described the site as a "fan site," with no commercial purpose. The site did, however, contain links to other commercial Web sites associated with the defendants. Taubman sued under the Lanham Act, claiming that the defendant's complaint site impermissibly infringed upon its trademarks. The trial court agreed and granted a preliminary injunction preventing the defendants from using the complaint site's domain names. However, on appeal, the trial court decision was reversed and the injunction dissolved. The court ruled that the defendants' calculated selection and use of Taubman's trademarks, even with specific intent to damage Taubman's business, did not constitute a commercial use of the trademarks. Thus, proof that a cybergriper's intentionally or actually causing the target company economic harm through the use of its own trademarks does not always lead to recourse for a trademark violation. If the defendant's use of the trademark is not in itself "commercial," then the Lanham Act provides no relief, regardless of the cybergriper's malicious intent or the degree of actual financial harm.

The judicial system is not the only government entity on the consumers' side with respect to e-complaining. The United States Department of Transportation since 1998 has collected e-complaints, particularly from air travelers. The Federal Bureau of Investigation in conjunction with the National White Collar Crime Center collects e-complaints on Internet fraud within the U.S., while the Federal Trade Commission accepts e-complaints on cross-border e-commerce (Millard, 2002). Likewise, the Securities and Exchange Commission set up a complaint center on its Web site so individuals can provide tips on financial reporting irregularities.

SOLUTIONS TO CYBERGRIPING

Pursuing cybergripers in court should be the last action taken against a cybergriper as it is time consuming and expensive. Further, the publicity from any lawsuit can be damaging to a business. We suggest that businesses consider arbitration or online dispute resolution (ODR) against cybergripers. ODR involves solving problems in an online forum. ODR represents a change in procedure rather than in substantive legal rights and liabilities of the parties, so it does not imply a legal right to recourse that does not already exist elsewhere in the law. Nonetheless, ODR appears to be gaining popularity and support through both free and paid services. In fact, some experts believe ODR will become the primary method of resolving disputes and claims that arise online (Solovnay & Reed, 2003). There are four major methods of ODR: (1) online arbitration, whereby all parties submit evidence and arguments online, and an arbitrator issues a decision; (2) online mediation, whereby a mediator facilitates negotiation and settlement in real time; (3) online ombudsmanship, whereby an online ombudsman reviews, investigates, and recommends a solution to the parties involved; and (4) online claim bidding, whereby a blind bidding of insurance and liability claims similar to an auction-type environment takes place. Sample providers of services of these different types of ODR include, respectively, adr.org, bbbonline.org, ombuds.org, and cybersettle.org.

Some of the early criticism of ODR is based on the lack of face-to-face communication, which is commonly thought to enhance the chances of conflict resolution. But in cases where the dispute arises online and in fact the entire relationship of the parties exists online, it seems unlikely that face-to-face contact, which would often be the first meeting of the parties, would fundamentally alter the chances of resolution. A greater threat to ODR is the problem of establishing which law controls the outcome of the case and which court has jurisdiction when a party seeks judicial enforcement of an ODR outcome. The overall effectiveness of ODR is more likely to be impacted by its ability to produce final, binding and enforceable resolutions than by its impersonal nature.

It may be best that hospitality and tourism businesses look first to tighten up their service recovery process; that is, use the prevention rather than the cure approach. Service recovery is an attempt to right past wrongs in an effort to correct a problem. The perceived fairness and effectiveness of handling the customer's complaint can significantly influence the success rate of service recovery efforts (Durvasula, Lysonski & Mehta, 2000), consequently increasing customer satisfaction, loyalty, and trust. Tyrrell and Woods (2004) contend that different levels of service recovery are needed depending upon problem severity (denial or delay), criticality levels (low -high), frequency of deviation (is it the first, second, or third time?), evaluation of prior attempts to fix; and compensation by company for problems encountered. Businesses must consider three key areas in service recovery, namely the ethical manner in which the problem is addressed; the time and expedience; and the level of atonement with which the problem is addressed. While these are not new, hospitality businesses are reminded that they cannot rest; rather, they must constantly seek to address guest complaints in order to avoid employee and consumer recourse at a later date. Though the business may eventually succeed in closing down the e-complaint site, this site is still available via such Web archiving sites as the Waybackmachine, located at Archive.org, a digital library with records of old Web sites.

Employers should begin with the old adage of seeing employees as internal customers. Employees, particularly those who engage in service recovery efforts for their employer, are more likely to expect better attempts by management to ensure that they are satisfied as well (Bowen & Johnston, 1999). In many companies, employers are expected to satisfy external customers in a manner similar to how they ensure workplace satisfaction. In a study of United Kingdom theme parks, research revealed that how the company goes about service recovery directly affects an employee's perspective of the company (Lewis & Clacher, 2001). In this study, it was found that employee intent to resign (quit) goes up with dissatisfaction of company efforts to recover service. When employees perceive the company as having limited intent to solve the customer's problem, employee turnover and absenteeism go up and loyalty goes down.

A disgruntled customer's act of establishing a Web site to berate a company is a relatively new phenomenon, but the impetus for that customer to act out is not. Research has shown that when customers perceive an establishment to have behaved unethically, they will often escalate the complaint behavior (Goodman, 2004). The extent of the complaint behavior depends on the gap between the customer's perception of how management should have handled the problem versus how management actually handled it. The cybergriper, who believes that he has been treated unethically, often feels justified in helping to steer customers away from an establishment. This is particularly true when the unethical behavior is practiced during the service recovery stage. Customers appear more willing to excuse unethical behavior during the service recovery stage if the initial problem could be considered extraordinary. For example, if a hotel employee were belligerent about a telephone charge for a call that never connected, the guest may perceive the business to be unethical, but perhaps not intentionally so. However, if the problem recurred, then the guest might believe that this unethical behavior was the norm. There appears to be a correlation between customer use of e-mail or telephone communications for service recovery efforts based on the extent to which the consumer perceives the company's effort as ethical or not (Alexander, 2002). If a company's response is unethical, or perceived to be so by customers, then customers are more likely to ramp up their complaint efforts. Perceptions of "being cheated" lead to the greatest reprisal activity.

Time is of the essence when dealing with customers, as they expect their problems to be addressed as soon as they are brought to the attention of the business. Customers get annoyed when relatively minor mistakes are not handled by front-line employees. Even if fervently working on a solution, the company must keep in touch with the customer; otherwise, the customer might become even more annoyed. This problem is particularly acute when the complaint forum is online. Complaints that are e-mailed to management are just as pertinent as

customer face-to-face complaints. It is easier for management to show the customer face-to-face that they are actively working on a solution to customer concerns. Prompt attention to customer e-mails is especially important, as half of all service recovery efforts will fail if customers feel that that they are being made to wait (Maister, 1985). Communicating that service recovery efforts are underway to the customer is very important. How service providers fill up "unfulfilled time" is an important consideration both in service delivery and service recovery (Maister, 1985). If customers perceive that they are being made to wait (with nothing to do while waiting), then it is likely that their perception of the service recovery efforts will be negative. The trick for companies is to respond effectively to online complaints in which there is not a face-to-face encounter. How does management convince customers that action is being taken? If the customer perceives that nothing is being done, service recovery will fail in approximately 50% of the instances. Likewise, expedience in recovery efforts and levels of atonement are also part of a customer's perception of a company's efforts at service recovery (Boshoff, 1997). The level of atonement in service recovery is described as the customer's perception of who in the company correctly solves their problem. For example, most customers want service delivery problems to be solved in one phone call or e-mail. When customers have to "ask for a supervisor" or seek a higher-level authority in the company to resolve their problem, their perception of company recovery efforts goes down, as does their level of satisfaction.

CONCLUSION

For companies the impact of cybergriping is far reaching. Cybergripers may act out of an altruistic desire to warn the general public about a target company's defective products or poor business practices or they may instead be motivated by the desire to coerce payment from the target company in return for closing the complaint site. Regardless, the risk posed by the cybergriper's site to the target company is the same: The potential loss of customers who are coaxed away from the target's official Web site to an attack site designed to deter the consumer from doing business with the target company. Moreover, cybergripers can reach anyone with Internet access. This may influence potential consumers around the globe for or against a corporation. Perhaps indicating the future potential reach of cybergripe sites are comments by consumer advocate Ralph Nader, who contended that complaint sites have the potential to become powerful political tools as they bring together people with common complaints who can then lobby Congress and state legislatures against corporate interests (Hearn, 2000). The Consumer Project on Technology has been petitioning since 2000 for Web domain name suffixes ".isnotfair," ".suck," ".customers," and ".complaints," dedicated to complaining online and thus making it easier for consumers and employees to find cybergripe sites and distinguish them from other sites (Ebenkamp, 2000). These domain name suffixes to date have not been approved and could change the landscape of the Web if they become available.

Harrison-Walker (2001) suggests some simple strategies for addressing cybergriping. These include forgetting about adopting anti-domain URLs; monitoring complaint forums and promptly responding to complaints; using specially trained representatives to handle complaints; and designing one's own complaint Web site or including an easy feedback mechanism in one's main Web site. In addition, management should develop an e-monitoring policy that governs employee Web use and the nature of what comments they would not be able to make online regarding the employer, fellow employees and customers. Off-duty use of computers, particularly those owned by the company, can be regulated (HRnext, 2000). When corrective action has been taken internally, be sure to update the customer and continually communicate improvements to the public. WorkingWounded.com, another site which allows employees to voice their complaints, suggests that employers not focus so much on one individual posting; rather they should look at themes that point to problems in the organization. If nothing else, see these forums more as focus groups with the potential to help the business improve (Simons, 2001; WorkingWounded.com, 2006). Bottom line: View e-complaints as valuable market

intelligence by paying attention to what employees and customers are saying about the company online, and respond in a positive manner (Harrison-Walker, 2001).

References

Abramson, J. & Hollingswood, C. (1998). Marketing on the internet--Providing customer

Satisfaction. *Journal of Internet Marketing* 1 (2). Retrieved March 10, 2006, from www.arraydev.com/commerce/jim/9802-01.htm.

Alexander, E. C. (2002). Consumer reactions to unethical service recovery. *Journal of Business Ethics* 36 (3), 223-237.

Appelman, H. (2001, March 4). I scream, you scream: Consumers vent over the net. *The New York Times*, p. 3.

Baldwin, I. (1999). Got a grievance? Gripe online. *Kiplinger's Personal Finance Magazine*, 53 (4), 20.

Band, J. & Schruers, M. (2003). Toward a bright-line approach to tradmarksucks.com. *Computer and Internet Lawyer* 20 (7), 1-15.

Bear Stearns Companies, Inc. v. Lavalle (2002), No. CIV.2.3:00CV1900D, 2002 WL 31757771, N.D. Texas.

Beetlestone, W. (2002). Litigation unique issues posted by defamation suits involving statements made via the Internet. *The Internet Newsletter* 7(4), 1.

Benderoff, E. & Hughlett, M. (2006, March 12). A whole lotta dissing going down on Web: Blog sites provide anonymous posters the opportunity to cybersmear their targets, and there's little you can do about it. *Knight Ridder Tribune Business News*, p. 1.

Beyette, B. (1999, November 2). Feeling a tad stressed over your job? *Los Angeles Times*, p. E1.

Booker v. GTE.NET LLC, et. al. (2003), No. 02-6190, United States Court of Appeals for the 6th Circuit, 350 F.3d515;U.S. App. Lexis 24452; 2003 Fed App 0427P, 6th Cir.; 149 Lab. Cas. CCH P59, 835; 20 I.E.R. Cas. BNA 1273.

Boshoff, C. (1997). An experimental study of service recovery options. *International Journal of Service Industry Management* 8 (2), 110+

Bowen, D.E. & Johnston, R. (1999). Internal service recovery: developing a new construct. *International Journal of Service Industry Management*, 10 (2), 118-131.

The Business Research Lab. (2004). Gold and silver employee satisfaction programs. Retrieved on March 6, 2006, from www.busreslab.com/consult/empsat.htm

Cohen, B. (1997). The "WOW" effect: How one restaurateur continues to delight customers, *Cornell Hotel and Restaurant Administration Quarterly*, 38 (2), 74-81.

Colden, A. (2001, January, 15). Corporations Increasingly Suing their Online Critics, Legal Experts Say. *The Denver Post*.

Douglas, A. C. & Mills, J. E. (2006). Logging brand personality online: Website content analysis of Middle Eastern and North African destinations. In M. Hitz, M. Sigala, &

J. Murphy, (Eds.), *International Federation of Information and Communications Technologies in Tourism*. Proceedings of the International Conference in Lausanne, Switzerland, January 18-20, 2006.Vienna: Springer.

DuCharme v. International Board of Electrical Workers, Local 45. (2001), Workers Local Union No. 45, No. 99-16310, United States Court of Appeals for the Ninth Circuit, 7 Fed. Appx. 633.

Durvasula, S., Lysonski, S., & Mehta, S. C. (2000). Business-to-business meeting service recovery and customer satisfaction issues with ocean shipping lines. *European Journal of Marketing*, 34 (3/4), 433-452.

Ebay, Inc. v. Bidder's Edge, Inc. (2000). 100 F.Supp.2d 1058, N.D. Cal.

Ebenkamp, B. (2000). Site for sore buyers. *Brandweek* 41 (25), 24.

Electronic Communications Privacy Act (ECPA), Pub. L. No. 99-508, 100 Stat 1848

Federal Trademark Dilution Act (FTDA) (1995) (15 U.S.C. 1125 et seq.).

Ferrera, G.R., Lichtenstein, S.D., Reder, M.E.K., August, R., & Schiano, W.T. (2000). *Cyberlaw: Text and cases*. Mason, OH: Thomson-South-Western.

Goldstein, M. (2003, September 14). Reputation of large companies subject to faster smear campaigns on the Internet. *New York Daily News*.

Goodman, J. (2004). Basic facts on customer complaint behavior and the impact of service on the bottom line. *Technical Assistance Research Program (TARP)*. Retrieved

March 6, 2006, from www.tarp.com/pdf/basicfacts.pdf

Grossman, L. (2003, December 22). Search and destroy: a gang of web-search companies is gunning for Google. *Time*, p. 46.

Harrison-Walker, L. J. (2001). E-complaining: A content analysis of an internet complaint forum. *The Journal of Services Marketing*, 15 (4/5), 397-412.

Hasbro, Inc. v. Internet Entertainment Group, Inc., 40 U.S.P.Q.2d 1479 (W.D.Wash. 1996).

Hearn, K. (2000, July 17). Gripe sites: consumers complain in chorus online. *Christian Science Monitor*, p. 15.

HRnext (2000). Privacy & cybergriping. Retrieved March 5, 2006, from http://www.vault.com/nr/printable.jsp?ch_id=402&article_id=53001&print=1 Retrieved

Intel Corp. v. Hamidi, No. S103781 (Cal. June 30, 2003).

Intel Corp. v. Hamidi, 1999 WL 450944 (Cal. App. Super., April 28, 1999).

Jackson, L.A. (2003, May). Have it your way. *Black Enterprise*, p. 110.

Kellner, L. F. (1994). Trade dress protection for computer user interface "look and feel." *University of Chicago Law Review* 61 (3), 1011-1036.

Konop v. Hawaiian Airlines, Inc. (2002), No. 99-55106, United States Court of Appeals for the Ninth Circuit, 302, F.Ed 868;U.S. App Lexis 17586; 170 L.R.R.M. 2906; 146 Lab. Cas. CCH P10,096; 19 BNA IER CAS 166; 2002 Cal. Daily Op. Service 7727.

LaMonica, M. (2002). Survey: employees ready to walk. Retrieved from www.news.com/2100-1017-98710.html

Lanham Act 3(a), 15 U.S.C. 1125(a) 1994 and Supp IV 1998.

Lewis, B. R. & Clacher, E. (2001). Service failure and recovery in UK theme parks: The employees' perspective, *International Journal of Contemporary Hospitality Management* 13 (4/5), 166-175.

Lockwood, R. & Nixon, C. (2005, Winter). [Your trademark]sucks.com: Protected expression or trademark infringement? *Trust the Leaders14*, 6-10.

Love, N. (2001). Customer service do you know its impact. Retrieved March 10, 2006, from www.lblconsulting.com/.

Maister, D. (1985). The psychology of waiting lines. In J.A. Czepiel, M.R. Solomon, & C. Superenant (Eds.), *The Service Encounter* (pp. 113-123). Lexington, MA: Lexington Books.

Millard, E. (2002, March). FTC web site goes global. *ABA Journal*, 88, p. 33.

Mills, J. E., Hu, B., Beldona, S., & Clay, J. (2001). Cyberslacking! A liability issue for wired workplaces. *The Cornell Hotel and Restaurant Administration Quarterly* 42 (5), 34-47.

Moebius, C. J. (2004). I can top that! Inside the world of employee complaint sites. Retrieved March 6, 2006, from www.bordercross.com/writing/watercooler.htm.

Newman, L. K. (2003). Cybersticks and cyberstones: Cybergriping after Bear Stearns and Taubman Company. *Internet Law & Strategy*.

Nunes, P.F. & Cespedes, F. V. (2003). The customer has escaped. *Harvard Business Review* 81 (11), 96-105.

Oasis Corp. v. Judd (2001). Case No. 00CV178, United States District Court for the Southern District of Ohio, Eastern Division, 132, F. Supp. 2d 612;U.S. Dis Lexis 2495.

O'Dell, S.M. & Pajunen, J.A. (1997). The butterfly customer: Capturing the loyalty of today's elusive consumer. Toronto: John Wiley & Sons.

Ponte, L.M. (2001). Throwing bad money after bad: Can online dispute resolution (ODR) really deliver goods for the unhappy internet shopper? *Tulane Journal of Technology and Intellectual Property* 3, 55-91.

Prosser, W.L. & Keeton, W.P. (1984). *Prosser and Keeton on Torts* (5th ed.). St. Paul: West.

Ramirez, N. (2001). Will the anticybersquatting consumer protection act create more problems than it solves? *Washington Journal of Law and Policy, Symposium on Intellectual Property, Digital Technology and Electronic Commerce* 8, 395-418.

Schlossberg, H. (1990). Satisfying customers is a minimum: you really have to delight them. *Marketing News* 24, 10-11.

Simons, J. (2001, April 2). Stop moaning about gripe sites and log on. *Fortune* 143 (7) 181- 182.

Singh, J. (1988). Consumer complaint intentions and behavior: Definitional and taxonomical issues. *Journal of Marketing* 52 (1), 93-105.

Sinrod, E.J. (2002). When a company sucks.com. *Corporate Counsel*, 2 (2), 96.

Snyder, P. (2004). Wanted: Standards for viral marketing. *Brandweek* 45 (26), 21.

Solovnay, N. & Reed, C. K. (2003). The internet and dispute resolution: untangling the web. New York: Law Journal Press.

Southerland, R. (2003). Go the extra mile today, keep employees loyal. *Atlanta Business Chronicle*. Retrieved September 13, 2005, from www.atlanta.bizjournals.com/atlanta/stories/2003/09/15/smallb2.html

Taubman Company v. Webfeats et al. (2003), 319 F.3d 770, 6th Cir.

Tyrrell, B. & Woods, R. (2004). E-complaints: Lessons to be learned from the service recovery literature. *Journal of Travel and Tourism Marketing* 17 (2/3), 183-192

Two Pesos, Inc. v. Taco Cabana, Inc. (1992), No. 91-971, Supreme Court of the

United States 505 U.S. 763; 112 S. Ct. 2753; 120 L. Ed. 2d615; U.S. Lexis 4533 60

U.S.L.W. 4762; 23 U.S.P.Q.2D (BNA) 1081; 92 Cal Daily Op Service 5571; 92 Daily Journal DAR 8910; 6 Fla L. Weekly Fed S 643.

Vail-Ballou Press, Inc. v. Tomasky (1999), 84500, Supreme Court of New York, Appellate Division, Third Department, 266A.D.2d 662; 698, N.Y.S.2d 98; 1999, N.Y. App. Div.

Varian Medical Systems, Inc. v. Delfino (2003), H024212, Court Of Appeal of California, Sixth Appellate Division, 113 Cal App. 4th 273; Cal. App. Lexis 1692; 2003 Cal. Daily Op. Service 9833.

Wilson, R. H. (2000). The law of cyberspace: Personal jurisdiction and the internet. *Cornell Hotel and Restaurant Administration Quarterly* 41 (5), 55-63.

Wolrich, C. (2002). The best corporate complaint sites. Forbes Magazine. Retrieved March 20, 2006 from www.forbes.com/home/2002/08/21/0821hatesites.html

Wolrich, C. (2005). Top corporate hate web sites. Forbes Magazine. Retrieved March 22, 2006 from http://www.forbes.com/2005/03/07/cx_cw_0308hate_print.html

Xuan-Thao, N. N. (2000). Should it be a free for all? The challenge of extending trade dress protection to the look and feel of web sites in the evolving internet. *The American University Law Review* 49, 1233-1283.

Juline E. Mills is Assistant Professor, Department of Hospitality and Tourism Management, Purdue University; **Brian J. Tyrrell** is Associate Professor, Hospitality and Tourism Management, Richard Stockton College of New Jersey; **William B. Werner** is Associate Professor, Harrah College of Hotel Administration, University of Nevada; **Robert H. Woods** is Professor, Harrah College of Hotel Administration, University of Nevada; **Michael S. Scales** is Assistant Professor, Hospitality and Tourism Management, Richard Stockton College of New Jersey.