



RICHARD STERN

r.stern@computer.org

Is mousetrapping unfair?

..... Like telemarketing at dinner-time, mousetrapping is one of those things you have to experience to appreciate. The frustration it engenders is part of what makes you decide whether you hate it enough to want to make it illegal. I can't give you that experience with the printed page, but I can point you toward a toned-down version of it.

I teach copyright and patent law relating to computer programs and the Internet at The George Washington University Law

School. Part of my pedagogical theory is that telling is insufficient in this legal field and must be supplemented by showing, to give students a proper appreciation of the issues. On the course's Web site, therefore, I've provided simulated forms of mousetrapping and related practices. If you want to experience some personal frustration of your own from mousetrapping, go to <http://www.law.gwu.edu/facweb/claw/Mousetrap1.htm>. By the time this issue of *IEEE Micro* reaches you, I

should have debugged the code enough for it to work. If not, you can e-mail me and tell me that I don't know enough how to write code to be a law school professor and that you do.

My mousetrapping isn't really mouse-trapping, anyway; it's more like mouse hindering. There are only a few alert boxes to grab your system, and they stop before you become infuriated. Real mousetrapping grabs control of your browser and won't let go. It grays out the back button and all back lines of dialog boxes (such as that for the Apps key on the bottom line of the Windows keyboard, between WIN and Ctrl). It can also disable the X box on the top right of your screen. Any attempt to escape just brings up the same or another pop-up window or alert box. Sometimes a flurry of Alt-F4 hits permits escape by closing the browser. Sometimes nothing but the three-finger salute (Ctrl-Alt-Del) works. Sometimes even that won't work, and the power-off switch is your only escape.

Mousetrapping gained public attention recently through litigation that the Federal Trade Commission (FTC) and enraged commercial victims have brought against several kings of Internet mousetrapping, notably John Zuccarini (sued for this practice over 60 times in recent years). These cases have focused mainly on trademark and unfair-competition theories of wrongdoing—as well as simple copying infringements under copyright law, because of the relationship of mousetrapping to



pagejacking. I consider these cases to be only the first generation of such litigation; a well-informed, ill-intentioned pirate can tailor conduct to avoid their applicability. A next generation of litigation will need to focus on possible copyright theories (mainly, unauthorized preparation of derivative works) that address the legality of someone comingling his own commercial content with that of an unwilling copyright proprietor.

How mousetrapping works

The simplest and least-effective form of mousetrapping is the alert box, a simple JavaScript pop-up window. You make one by inserting special code, like that in Figure 1, into your Web page's HTML code.

You can string together as many lines of alert messages as you want. When the user closes one box, the next one will pop up, until they have all displayed. You could even make the last alert message in one set trigger a second set, and have this set's last alert message send users back to the first set. But this would be pointless, and you certainly wouldn't sell any merchandise that way.

A commercial mousetrap is less blatant and overt. It is an interlinked system that basically works like the simplified block diagram in Figure 2 indicates.

In this system, which the mousetrap simulation on my site follows, you enter an introductory page (Intro Page) maintained by a mousetrapping entrepreneur. Intro Page contains JavaScript that transfers you to the entrepreneur's, or his client's, commercial site page (Site Page 0). This transfer occurs after a predetermined delay interval—or, if less blatant, through a mouse click induced by promises of free samples (my demo mentions free term papers; porn kings make other offers). Once you reach Site Page 0, the back functions no longer work. Any efforts to leave Site Page 0 by closing the browser window just transfer you to Site Page 1, Intro Page, or another such site. Likewise, if you try to leave Site Page 1 by closing the

```
<HTML><head> ...
<SCRIPT language=JAVASCRIPT>
<!--
function AlertBox(){
  alert('Purchase my stuff, NOW!');
  alert('I mean it, buy NOW!!!');
  alert('This is going to keep going until someone like the FTC brings a lawsuit
  to make me stop it! OK?');
}
-->
</script>
</head>
<body onload='AlertBox()>
... </body></html>
```

Figure 1. Example HTML code for alert boxes.

browser window, you end up at Site Page 2. Efforts to leave Site Page 2 send you back to Site Page 0, and the cycle continues indefinitely (unless the mousetraper programmed compassion into the JavaScript—not very likely—or your system crashes from loss of memory). Users of a real mousetrap system can leave any initial site page, however, by clicking on a link to a deeper level of the same site, such as one calling for payment for viewing.)

My demo system, unlike the commercial ones the FTC is proceeding against, has just three site pages, because I did not want to write and debug any more code than that. (At my Web site, you can see the code for this system and for two of Zuccarini's systems; his code is much better, because he can afford the best JavaScript writers in the world, and I can't. I invite you to contribute your codes by e-mail, because I am planning to establish a mousetrapping archive at the site as part of figuring out what ought to or ought not to be suppressed by law.)

FTC's Zuccarini suit

As explained in *FTC v. Zuccarini*, 01-CV-4854, E.D. Pa., the FTC challenged the

defendant for registering URLs with misspelled versions of famous persons' names (such as "BritnaySpears.org"), trademarks (like wallstreetjournal.com), or cartoon characters (for example, he registered "dillbert.com"—with two l's). A partial catalog of Zuccarini's misspelled-word URLs (<http://www.keytlaw.com/Cases/zuccarini'scases.htm>) shows dozens of cybersquatting proceedings against him and his companies.

Thus, if someone seeking Microsoft mistyped "Microsof," or someone seeking the Computer Society mistyped "IEEComputerSoceity," the person's browser might download a site with some unexpected content. In some cases (for example, in a pagejacking and mousetrapping suit that the FTC brought in 1999), pagejacking causes search engines to direct browser users to one of these sites. Because the pagejacked page's metatags are copied along with the rest of the pages' content, Google and other search engines think it's just another site addressing the metatagged topics. (If that happens, no misspelling is needed.) Zuccarini has placed metatags naming film stars in his code, and also nonprinting code where search engines will find it (for

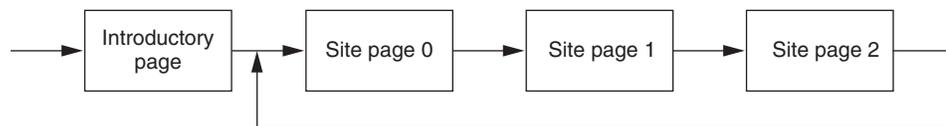


Figure 2. Simple mousetrap system.

```

<P>WARNING! This site contains . . .
<P>But I declare that I do not object to explicit images of . . . or find them
offensive.
<P>I take full responsibility for my actions.
<P>I hereby release and discharge the providers, owners, and creators of this
site from any and all liability that might arise.
<P><a href="URL of notional VileSite.com" target="_parent">I agree to the
above and want to PROCEED!</a>
<P><a href="URL of notional EvenVilerSite.com" OnClick="goback=false">I
disagree and want to DEPART</a>

```

Figure 3. Example source code for a mousetrap. Whichever option you click, you get mousetrapped at a target site, either VileSite or EvenVilerSite.

example, keeping the text color the same as the background screen color). In his page source code, he sometimes spells the same names correctly and then incorrectly. One way or another, the viewer stumbles into a Zuccarini site (comparable to the Intro Page of the system shown earlier).

Once you reach the Intro Page, JavaScript code redirects you to a URL and regular site of the client advertiser, who pays Zuccarini 10 to 25¢ for capturing and redirecting each potential customer. (This amount is a very high price for a hit, giving an idea of how much money this business may involve.) Zuccarini retains the site on which the JavaScript capture and transfer occurs so that it can be used for another client advertiser if the present one moves on. After redirection, something like the demo just described occurs. You are offered porno samples and invitations to check more of the same, or solicitations for online gambling, lotteries, psychics, credit cards, and so on. Once again, just clicking on the back or X buttons will not release you. You are mousetrapped.

A curious byproduct of researching for Micro Law put me into the path of a particularly obnoxious example of this practice. As part of my research, I signed up for a World Wide Consortium e-mail discussion group. Immediately, I started getting spam for porno sites. Aha! This gave me an opportunity to check out their source code to see how they did it. One of them ticked me off so much that I was ready to sic the FTC on them (I would have had a field day out of this 40 years

ago when I worked at the FTC), until I noticed that their site was based in the Czech Republic—I don't think the Czechs will extradite anybody for the FTC. Figure 3 gives you an idea of the source code for such a mousetrap.

What are unfair acts?

Still, it takes more than getting people mad to make a business practice "unfair" according to the FTC Act. What makes this conduct unlawful? The FTC proceedings against Zuccarini and other mousetrappers differ from those brought by Dow Jones (*Wall Street Journal* case), United Feature Syndicate (*Dillbert* case), and other private intellectual-property (IP) litigants. Section 5 of the FTC Act authorizes the FTC to suppress unfair or deceptive acts and practices. The FTC has thus proceeded more broadly than trademark owners have.

As the FTC's complaint against Zuccarini and its legal memorandum in an earlier similar case indicate, the FTC considers pagejacking and mousetrapping to be both deceptive and unfair. They are deceptive for largely the same reasons that trademark owners' suits have been successful: confusing the public as to the advertiser's association with or sponsorship by the trademark owner.

More important, a practice is unfair, for purposes of section 5 of the FTC Act, if

- the practice causes, or is likely to cause, substantial injury to members of the public;
- the public cannot reasonably avoid that injury; and

- substantial countervailing benefits to competition or consumers do not outweigh the injury.

According to the FTC's complaint against Zuccarini, the claim of unfairness rests on the following:

- Consumers incur transaction costs, including Internet connection fees, lost time, and lost data (presumably from crashes).
- The practices expose children to solicitations for pornography, gambling, and psychics.
- Employees are trapped into visiting porno sites, which may get them into trouble with their employers. (One of Zuccarini's pages offers users a \$70 Internet Eraser utility download to help conceal porno surfing from employers.)
- Consumers are hindered from visiting the Web sites they desire to visit. This impairs the Internet's growth, contrary to the public interest.

District court rules for FTC

The district court found that there was good cause to believe that Zuccarini violated section 5 and that the FTC was therefore likely to prevail based on the case's merits. The court determined that a temporary restraining order (TRO) was in the public interest, and it entered the requested preliminary relief, which Zuccarini did not show up to oppose. (He is rumored to be hiding out in Florida, grumbling all the way to the bank where he counts up the \$1 million per year that the FTC estimates he's been making from his advertiser clients.)

The TRO orders the defendant to stop mousetrapping consumers and to stop operating Web pages with URLs that are misspellings of other names or terms. In addition, the court orders Zuccarini to close down his Web sites with various-named URLs, unless and until he brings them into compliance with the TRO requirements that the district court issued against him at the FTC's request. The order lets him reopen and resume opera-

tions if he brings the sites into compliance. But because that would destroy his business model, it would seem to be quite a challenge for Zuccarini to refurbish his operation in accordance with the order. (Presumably any final order would have similar provisions. The FTC also wants to compel payment of restitution as part of any final order.)

Zuccarini on linking

Curiously, Zuccarini is a copyright theoretician in addition to his other interests. In the *Wall Street Journal* case, he got into a dispute with Dow Jones (owner of *The Wall Street Journal*) and the URL regulatory body (the World Intellectual Property Organization) over the legality of linking. Dow Jones accused Zuccarini of providing links on his sites to the sites of other businesses, such as a credit card company and presumably *The Wall Street Journal*. Apparently, Dow Jones objected to the links on the basis that, by itself, or perhaps in conjunction with his use of the "Journal" misspelling for his site, the linking created public confusion as to who sponsored or was associated with Zuccarini. Dow Jones sought to draw the conclusion that this confusion because of his use of links was another reason to extract the Journal URL from him and to transfer it to Dow Jones (as eventually occurred). Zuccarini indignantly and articulately responded:

To say, even if I did have links to the *Wall Street Journal*, I would need to be authorized by them to have these links is outlandish. I do not need permission from the *Wall Street Journal* to link to their Web site from any Web site I own. That is my right. The Internet is much more than just links, but if the Internet is anything, it is millions and millions of pages with links on them. Is the *Wall Street Journal* proposing that these millions and millions of links [must] all have official authorization?

The weight of commentary and such

little precedent as now exists probably favors the quoted passage. Linking, at least per se, is not infringement of IP rights, is privileged, and is socially beneficial. Use of the Internet—and Internet research in particular—greatly depends on the legality of linking without specific permission.

Changing the facts

Mousetrapping represents perhaps the polar extreme of obnoxious Internet marketing and advertising behavior. It may be even more obnoxious than spamming. Nonetheless, mousetrapping per se may not implicate IP law, and may not even violate FTC Act section 5 in all circumstances. For example, consider a case without the porno aspect. Or consider mousetrapping that impairs the back function but not the X button. Or what if a site limits its mousetrapping to a few pop-ups, as in the alert box demo at the beginning of my Web page on mousetrapping? Is there still substantial, unavoidable consumer injury if the facts change as just described? The FTC's unfairness analysis in *FTC v. Zuccarini* and similar cases might then no longer hold.

Furthermore, assume there is no pagejacking or similar deceptive conduct. (There apparently was no pagejacking in *FTC v. Zuccarini*, although pagejacking was a component in prior FTC litigation against mousetrapping.) In this instance, does the FTC's case, as modified, become a farfetched, hypothetical argument? Maybe, because Zuccarini's business model probably depends on some degree of coercion and oppression of users. Normally, a seller cannot mistreat customers very much and still keep their business. (Suppose Wal-Mart locked the store door and wouldn't let you out until you bought something. Would you ever come back?) Porno sites are different. They apparently do not depend on repeat trade from satisfied customers. Instead, they base their business model on very short-term gains made from one-time customers by sellers who remain indifferent to the sensibilities of exasperated, resentful, mousetrapped consumers. It

could be that letting the user off more easily would stop the system from generating such high revenue; 25¢ per redirection is a very high rate by current standards, but these sites apparently can afford it.

Moreover, not all mousetrappers lead users to porno sites (even Zuccarini's clients included a credit card company). In fact, mousetrapping, and conduct very much like it, is pervasive on the Internet. Some of the most well-known corporations practice it, presumably because they think it pays off. For these advertisers, the "kindler, gentler" mousetrapping scenario is not far-fetched.

These practices help marketers induce customers to purchase their products. A key element in this marketing system is getting the user to the site and making him hold still long enough for the advertiser to expose the user to advertising. Perhaps the wait evokes some mouse clicks, putting the advertiser's product into the user's shopping basket. (If the broker who forwards the user is a third party, rather than the product seller itself, the seller pays the broker for the hit.) Almost every business on the Internet does something like this to some degree. That's why you see all of those links to Amazon.com everywhere and why search engines display targeted advertising based on customer queries.

Not all of this is coercive enough to earn the mousetrapping label. But a surprising amount of it is. Table 1 (next page) gives a short list of more or less reputable companies that keep you mousetrapped on their Web pages. I have provided links so that you can form your own judgment as to whether they are mousetrappers. Their scripts either keep you on the same page indefinitely and refuse to let you go, or put up different successive screens if you don't want to buy whatever they want to sell you on the first screen—for example, endlessly offering subscriptions to different magazines ("More Great Deals!") in the hope that you'll finally find one you like. The scripts perform differently on different browsers; some browsers are harder to trap.

Table 1. Some of corporate America's Web site mousetrappers.

Company name	Browser*	Link	Business description
PepsiCo	Netscape 4.6	http://www.pepsi.com/current/pepsistuff_2001/link_home2splash.html	Beverages
Digital River	Internet Explorer 6.0	http://drhome.digitalriver.com/livehtml/newsite/dr_home_flash_main.html	E-commerce marketing consultant
MagazineOutlet.com	Internet Explorer 6.0	http://www.magazineoutlet.com/magoutlet	Magazine subscriptions
Kellogg	Internet Explorer 6.0, Netscape 4.6	http://kelloggs.com/eetnern/eehome/index.html	Cereal, snacks

*The given site mousetrapped me when I used the listed browsers.

Mousetrapping and pagejacking defined

The following definitions and information are from the Marketingterms.com Marketing Dictionary (<http://www.marketingterms.com/dictionary/>).

Mousetrapping

Definition. The use of browser tricks in an effort to keep a visitor captive at a site, often by disabling the "Back" button or generating repeated pop-up windows.

Information. Mousetrapping is one of the most extreme marketing tactics on the Web. The goal is to extract maximum value from one-time visits, typically by bombarding visitors with a never-ending supply of traffic-exchange banners and pay-per-click links. Extreme forms of mousetrapping are often found on the "red-light district" of the Web, where precious little consideration is given to repeat visitors. Since these sites cannot count on repeat visits from satisfied visitors, they often resort to deception to acquire new visitors. Mousetrapping comes in many varieties. The most mild form of mousetrapping involves disabling the "Back" button. (Note - not all broken "Back" buttons are a result of intentional mousetrapping; some are the result of scripting routines used for other purposes.) More aggressive forms of mousetrapping include disabling of key browser features and continuous loading of pop-up ads.

Pagejacking

Definition. Theft of a page from the original site and publication of a copy (or near-copy) at another site.

Information. Pagejacking does not mean taking over a page on the original site. In fact, the original site can be completely unaware that the theft has occurred. Pagejackers siphon off traffic indirectly through the search engines. The stolen pages are copies or near-copies of the original pages. The stolen pages are then submitted to the search engines in an attempt to duplicate the rankings of the original pages. After the pages are submitted, the stolen pages are switched in favor of pages which [sic] learn revenue for the thieves. To further complicate matters, sometimes cloaking is involved.

For a more extensive list, see Top9.com's lock-in list (<http://www.Top9.com/lockin.html>), where I found the information listed in Table 1.

In some cases, the corporate seller does not itself capture the viewer in the first instance. For example, the Kellogg's mousetrap site is for viewers redirected

to it from the Cartoon Network (AOL Time Warner). The Cartoon Network redirects viewers to the Kellogg's site in essentially the same manner that Zuccarini redirects viewers to his clients' sites, and presumably for a payment. The more you study this situation, the more all these sites seem the same, or at least they

appear to be more on a continuum, rather than a case of good guys and bad guys.

Getting the user to a JavaScript

So what's going on here? The idea is to get the user to a Web page (corresponding to the Intro Page in my mousetrap demo) in which the system operator can include his own JavaScript or similar code. To mousetrap a user, the mousetrapper needs to get his own code into RAM on the user's computer, to control the displays on the computer and maintain the trap. Is this unfair per se, for purposes of FTC Act section 5? Probably not, at least under the current legal standard invoked in the Zuccarini case. The examples in Table 1 lack the elements that put the FTC's cases "over the top" against its adversaries. There is no pornography or overt false representation about sponsorship. The substantial and unavoidable injury to consumers alleged in earlier FTC cases appears to be missing. There is just some annoyance, some very bad netiquette. Probably, having a hundred successive magazine subscription offers jammed up your nose before you pull the plug on your computer won't stifle the Internet's progress. (Actually, it usually isn't even that bad or unavoidable, because most of the sites let you hold the browser's back button down to select and escape to a much earlier page. Unlike Zuccarini's pages, these do not essentially say, "All your back functions belong to us.")

But how does a company get users to a JavaScript, preferably without unduly

antagonizing them? Most of the sites attract its customers by whatever ordinary means it used in the past. The site uses JavaScript to hold the users for a little longer, to make the site stickier. The Kellogg's site attracts users with the copyrighted cartoon content that the Cartoon Network provides (for a fee). Kellogg licenses these cartoon characters, and so does not infringe copyright.

What else could a company do to get similar results? It could use inline framing (iframing), or framing in general, which are ways to create a Web page that seems to contain somebody else's Web page as a component of the company's Web page. The other page is linked to the company's page in the same way that you might link an image from somebody else's site. For a demonstration of the most complicated framing you are ever likely to see, visit <http://www.law.gwu.edu/facweb/claw/Ad'frame.htm>. For links to articles and other materials on framing, see <http://www.law.gwu.edu/facweb/claw/framing.htm>. Using iframing is a way to get users to a page on which the company places its own code to seize control of the user's computer. The company could iframe some material from a cartoon site, as the Cartoon Network does for Kellogg. However, must the company pay the owner of the copyright in the cartoon for doing so? That is, is it copyright infringement to use a cartoon (say, Dilbert or Snoopy) in a frame without paying for a license?

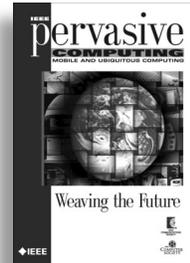
Still another method would be a Trojan horse strategy. A company could lure the user into installing a program that alters Web pages the user visits, so that those pages display the company's pop-up advertisements or links to predetermined Web pages. The company could bundle this program with a free application, such as a Napster or Gnutella substitute. (Ezula made such a deal with Kazaa.) Once a company has an installed base, it's in business. Say Ford pays a company to sabotage GM this way. Ford would be paying this company for the word "car." The company's software would place links to the Ford Web page at every point on the GM

Web site (as viewed by users of the Trojan horse program) where "car" occurred. Friends and users of this technique call it *contextual advertising*; detractors call it "scumware" (see <http://www.scumware.com>). I'll elaborate on the copyright/copywrong aspect of this technique in a future Micro Law column. Like iframing, contextual advertising raises novel, difficult issues about when a derivative work (a modified version of an earlier work) is an unlawful invasion of the original copyright owner's rights.

A considerable amount of inconclusive litigation and conflicting authority cover these points. None of it gives a definitive answer. For example, one federal appeals court in Los Angeles (the *Mirage* case), says razor-blading a drawing from a book, placing the drawing between two sheets of plastic or glass, and taping the edges together is copyright infringement, whereas a federal appeals court in Chicago (the *Annie Lee* case) says the opposite. Of course, the copyright and copywrong of framing Internet content is even more complicated legally than framing pictures. Courts and lawyers have been trying to figure out this issue for years. If they ever do, I'll tell you in Micro Law.

Various demos at my George Washington University course Web site show that it is possible to place your own HTML code on a page that frames or otherwise uses another's content. The net effect is to let the subsequent page's operator associate its advertising material with the other person's content, while using the other's content as bait for users. Unless the courts deem this the unauthorized preparation of a derivative work, as the *Mirage* case somewhat questionably indicates, copyright law does not provide a remedy. It is simply, to use a term of art, tough luck. As the *Annie Lee* decision's rejection of *Mirage* tells us, not every collocation or juxtaposition of copyright-protected material is a preparation of a derivative work. What remains to be developed is a theory of copyright law liability that could satisfactorily resolve these issues. I plan to take a stab at that.

**NEW FOR 2002,
the IEEE Computer
and Communications
Societies present**



**IEEE
Pervasive
Computing**

This new quarterly magazine aims to advance pervasive computing by bringing together its various disciplines, including

- hardware technology
- software infrastructure
- real-world sensing and interaction
- human-computer interaction
- systems considerations such as scalability, security, and privacy.

Led by Editor in Chief M. Satyanarayanan, the founding editorial board features leading experts from UC Berkeley, Stanford, Sun Microsystems, and Intel.

**Don't miss the
premier issue —
subscribe now!**

<http://computer.org/pervasive>

