
Invisible Ink: When What You See Is Not What You Get

2001-09-26

A recent lawsuit shows how far web sites will go to elbow their way to the top of Internet search engine results. In June, a Belgian company sued Women.com Networks for copyright infringement and unfair trade practices. The Belgian firm, Euregio.net AG, runs a directory of horoscope sites called EasyScopes.com. The firm alleged that Women.com copied a paragraph of text from the EasyScopes.com horoscope directory and posted the text on its own astrology site at InternetHoroscopes.com. The twist, however, is that Women.com posted it as invisible text: white letters on a white background. The purpose? To boost the site's position on search engine results.

White-on-white text is the latest in a series of controversial techniques used by web sites to improve their search engine standings. In the past, web sites have attempted to increase hits by manipulating meta tags, which are part of a web page's HTML code and are used by search engines to index sites. Although meta tags are designed to refer to the subject matter of the site, some sites use unrelated words or trademarked terms in their meta tags to attract more search engine users. Courts have generally looked askance at this behavior. As discussed in our [April 2, 2001 Internet Alert](#), the Seventh Circuit has held that use of third party trademarks as meta tags can demonstrate an "intent to cause confusion," which is a factor that many courts consider in assessing a "likelihood of confusion" - the legal standard for infringement. Playboy also obtained a [preliminary injunction](#) against a site that used the term "playmate" in its meta tags. Furthermore, other courts have granted preliminary injunctions for deceptive trade practices against companies that placed false information in their meta tags to induce consumers to visit their sites.

Even as the case law against meta tag "abuse" develops, web sites are turning to new methods of tricking search engines. Some web sites embed an unused frame, which contains terms invisible to web surfers but visible to search engines, in their pages. Other sites bury search terms in a "bridge page" that users view only momentarily before being automatically redirected to the actual site. Still other sites use a technique known as cloaking, or "pagejacking," in which a search engine spider is given a different version of the web page than what a human visitor would see. One pagejacker, against whom the FTC has successfully sought a [preliminary injunction](#),

copied the contents of popular web pages, submitted them to search engines in place of the true contents of his page, and sat back to collect hits from misdirected users who had been searching for one of the popular sites. In addition, search engines themselves often sell popular search terms

and names to companies desiring higher placement in search results.

Another recent practice involves the use of nearly invisible monitoring devices which are hidden on web pages in tiny graphics files that are often only one pixel in dimension. These "web bugs," "1x1 GIFs" or "pixel tags," as they are sometimes known, are invisible to a web site visitor. However, they can provide information about the user's site visit, IP address, browser type and cookies to third parties such as Internet advertising networks. Web bugs have recently become the focus of privacy advocates, and have been challenged by the Michigan Attorney General, who argued that the privacy policies of four online retailers did not adequately disclose the use of these devices.

As these forms of "invisible" publishing become more sophisticated, users of the Internet and owners of intellectual property must become more vigilant in efforts to protect their privacy and their property against unseen tampering, appropriation and tracking.

Jorge Contreras
jorge.contreras@haledorr.com

Michael Bevilacqua
michael.bevilacqua@haledorr.com

Contributions to this article were made by summer associate Rita Lin.