

## Client Advisory

October 2002

# Are Your Trade Secrets and Proprietary Property Available for the Taking In Cyberspace?

Too frequently, many companies' secrets and other valuable information and materials, stored as electronic data, are easily accessible in cyberspace. Every company — as part of a comprehensive trade secrets and intellectual property protection program — should audit its MIS and computer policies and procedures, and those of its vendors and other third-parties that handle sensitive company information. In addition, companies often mistakenly rely on intellectual property law to protect databases and certain other valuable information posted on Web sites that may, in fact, have limited, if any, protectability at law.

This KMZ Rosenman client advisory explains some of the steps to safeguard your digital property and explains what remedies may be available if sensitive data is procured and disseminated without authorization.

### **Beware Hackers, Spiders, Bots and Other Threats**

The Internet is a network of connected computer systems. Your company's Web site and its computer systems are connected, directly or indirectly, to the Internet. This makes the data, including information you deem confidential, proprietary and trade secrets, subject to potential access and procurement by your competitors, trade journalists and other unauthorized parties.

Most people have heard of the dangers posed by hackers, those nefarious computer geeks who gain unauthorized access to targeted computer systems. Still, companies frequently make sensitive data all too easy to find and procure. A person seeking digital information of interest — research and development specifications and results on your next generation of a key product, for example — need not specifically target any one computer system. So-called spiders, bots and other intelligent search agent programs scour the Web every day in an effort to find specific accessible data in Web site and other HTML files. In some instances, search agent programs even dig into non-public files located on the same server or connected servers as public files, which are not sufficiently protected by network security, such as firewalls and password-protected areas. If you have ever used Google™ to perform a search, you have employed a form of this technology.

Even if your company's MIS department has employed state-of-the-art network security systems and trained your staff to follow good security protocol, it is likely that your company has entrusted valuable information to its vendors (and your vendors' vendors), some of which may not be employing sophisticated security systems and policies and procedures. In addition, your Web site may include information that is not confidential but that you do not intend to be systematically collected and then used for commercial advantage by third parties — a task that is easily accomplished by spiders and bots. Finally, links to, or URLs of, digital files in emails or on public files may provide unintended parties with access to files you thought were private. A number of steps can be taken to protect your company from these types of unauthorized or unintended access and data collection.

## **Security Policies and Procedures, Vendor Codes of Conduct and Terms of Use**

The first defense against unauthorized and unintended third-party access to your sensitive files and systems is good network security policies and procedures. This includes not only the use of firewalls and password-protected areas, but education about the policies and procedures and exercise of best practices by all employees and vendors. Centralized authority through your MIS Department helps to maintain control. For instance, no person should be permitted to add to or change the company Web site or post HTML files or links without clearance from an MIS supervisor.

If your company uses vendors and other third parties that deal with your confidential, sensitive or valuable information, it is equally as important that they exercise the same kind of care as you do in maintaining the security of their systems and the information. Most companies include confidentiality clauses in vendor contracts, and many require formal non-disclosure agreements and even acceptance of non-disclosure obligations by signing reception desk visitor logs. Companies concerned about their corporate image, goodwill and trademarks often require vendor codes of conduct that prohibit illegal activity, disparagement and controversial practices, such as use of third world "sweat shop" labor. KMZ Rosenman, in association with clients in the technology and advertising industries, have developed a form of vendor code of conduct requiring use of best practices regarding protection of sensitive information and computer security. It is recommended that all companies consider similar vendor requirements.

In addition, your company's Web site Terms of Use should specifically prohibit use of bots, spiders or intelligent agent software (or other methods) for any purpose other than accessing publicly posted portions of the site and then only for the purpose of a limited, noncommercial single-computer use. The Terms of Use should state that the user agrees not to, and not attempt to, circumvent any access or use restrictions, date encryption or content protection; not to data mine and not to in any way cause harm to or burden the site. As discussed below, courts have found use of a site in violation of its Terms of Use to be actionable as breach of contract. KMZ Rosenman maintains sets of Web site forms for most applications and constantly updates them to address emerging issues and developments in the law.<sup>1</sup>

Finally, your company's site can employ a standard for robot exclusion, a device that permits you to give express consent or denial to bot/spider access to specific Web pages. A "robots.txt" file is placed in the directory of a server, and search programs that are designed to look for and respect exclusions will not access excluded files. While spider proprietors who do not respect this growing industry standard will still be able to access excluded files, accessing excluded files is evidence of trespass.

## **Wrongful and Unintended Data Collection and Use May Be Subject to Various Legal Claims**

Your data may be capable of copyright or trademark protection, thereby giving your company the exclusive right to reproduce, display, publish and otherwise exploit the data. However, this protection is not without exception, and each circumstance will need to be individually considered.

For instance, some use of copyright protected material may be considered a fair use. *Compare Kelly v. Arriba Software Corp.*, 77 F.Supp.2d 1116 (C.D. Calif 1999)(collection of images by bots was fair use under copyright law for the transformative purpose indexing websites), *with, Playboy Enterprises Inc. v. Webbworld, Inc.*, 991 F.Supp. 543 (N.D. Tex 1997), *aff'd mem*, 168 F.3d 486 (5th Cir. 1999)(copyright infringement found where bots programmed by a commercial site to collect protected images from postings on newsgroups). Further, not all information treated as proprietary is capable of protection under copyright or trademark law. For instance databases and collections of public information, even if valuable to you once collected, are subject to minimal, if any, protection. Indeed, the originality of the selection and arrangement of the contents of a database will dictate whether or not the database is entitled to protection.

---

<sup>1</sup> Prior Client Advisories and articles by Mr. Friel discussing Terms of Use and other Web site legal issues are available upon request.

There is currently pending legislation attempting to protect databases. The Collections of Information Antipiracy Act, H.R. 354 106th Cong. (1999), seeks to protect qualifying databases by prohibiting specific uses and extractions of information that cause commercial harm to the actual or potential market of the database's owner. Under the proposed bill, misappropriation could occur if a relatively small but crucial portion of the database is used or extracted. Remedies for violation are proposed to include injunctions, impoundment of misappropriated information, monetary relief and criminal sanctions for willful violation. However, the Collections of Information Antipiracy Act remains unenacted.<sup>2</sup>

If the bill, as it stands, is enacted, the law and its remedies may provide a solution to the problem of certain common forms of Internet trespass. Conduct such as "deep linking" (see [Ticketmaster Corp. v. Ticketmaster.com](#), discussed below) could be misappropriation under the Collections of Information Antipiracy Act if the Court finds that such linking constitutes use of a viable portion of the owner's database. However, until enactment of the Collections of Information Antipiracy Act, trade secret law may provide protection so long as you take reasonable steps to keep the information confidential and non-public (e.g., completely non-public or available only by subscription and subject to non-disclosure obligations). Poor policies and sloppy practices regarding computer security will work against your ability to enforce trade secret laws. Further, if it is essential that the information be freely and publicly available, trade secrets law will be of little avail.

If it can be shown that the data was accessed, through the use of bots or otherwise, by a person who "exceed[ed] authorized access and obtain[ed] information that it is not entitled to obtain[.]" then that person is potentially liable under the Computer Fraud and Abuse Act. 18 USC Sec. 1030(a)(2)(C); see also Sec. 1030 (a)(5)(C) and 1030(e)(8)(unauthorized access that causes damage). In this regard, exclusions in your Web site Terms of Use and use of robot exclusion standard files are important to establish what access and use is permitted and what is unauthorized. In [Register.com v. Verio, Inc.](#), a federal district court enjoined Verio's use of bots to harvest domain names from Register.com's Web site and to then solicit those users for competitive services under a number of causes of action, including Section 1030. 26 F.Supp.2d 238 (S.D.N.Y. 2000). The Court in Register.com also issued the injunction on the grounds that the plaintiff was likely to prevail on its breach of contract claims and its trespass to chattel claim. The breach of contract theory was based on the bots' collection of, and Verio's use of, data from Register.com's Web site in violation of that site's posted Terms of Use.

Trespass to chattel is an old English common law doctrine that now exists under state law. The Restatement (2nd) of Torts Sec 218, followed by most states, requires the owner to show one of the following: 1) the defendant dispossessed the owner of chattel; 2) the defendant impaired the chattel's condition, quality or value; 3) the owner was deprived of the use of the chattel for a substantial amount of time; or 4) some person or thing in which the plaintiff had a legally protected interest was harmed. Several cases have been reported where this theory was applied against parties employing bots or spiders on commercial Web sites. See [eBay Inc. v. Bidders Edge, Inc.](#), 100 F.Supp.2d 1058 (N.D. Cal. 2000)(use of bots caused "intermeddling with or use of another's personal property" and thus trespass to chattel); [Register.com v. Verio, Inc.](#), 126 F.Supp.2d 238 (S.D.N.Y. 2000)(absent consent to bot usage, bots are an unwelcome interference with, and a risk of interruption to, computer systems and servers). An unreported trial court decision, which was upheld by the 9th Circuit without written opinion, failed to permit a trespass to chattel cause of action for Tickets.com's accessing of Ticketmaster's Web site to publicly copy a posted database of event information. [Ticketmaster Corp. v. Ticketmaster.com](#), Civil Action 99-7654 HLH (BQRx), 2000 US Dist LEXIS 12987 (C.D. Cal. Aug 10, 2000), aff'd mem., Appeal No. 00-56574 (9th Cir. Jan. 2001). In that case, the court found insufficient "physical harm to the chattel ... or some obstruction to basic function...." However, the court seemed influenced by the fact that the appropriated content fell short of copyright protection (a listing of facts — concert dates): "Thus, unfair as it may seem ..., the basic facts [that Tickets.com] gathers and publishes

---

<sup>2</sup> On January 19, 1999, the Collections of Information Antipiracy Act, H.R. 354 106th Cong. (1999) was referred to the House Committee on the Judiciary. As of 2002, the Bill remains before Congress.

cannot be protected from copying.” Accordingly, this case may not reflect how courts would treat access and appropriation of clearly confidential information or copyright-protected content. For other related cases, *see also* Thrifty-Tel Inc. v. Beznec, 54 Cal.Rptr.2d 468, 471 (Cal. App. 1996)(hacking of computer to place long distance calls was trespass to chattel even though the electronic signals were intangible); Compuserve Inc. v. Cyber Promotions Inc., 962 F.Supp. 1015 (S.D. Ohio 1997)(spamming can be trespass to chattel).

□

Depending on the facts, there might also be a claim for violation of the anti-circumvention provisions of the Digital Millennium Copyright Act, 17 USC 1201, which prohibits circumventing copyright access controls. For instance, if robot exclusion standards (robots.txt), file access systems, firewalls, encryption, etc. are circumvented, this additional cause of action might be a viable claim.

## We Can Help

Companies need to review their policies and practices and those of their vendors and other third parties that they entrust with sensitive and proprietary information. KMZ Rosenman is experienced in helping its clients conduct an audit of their policies and procedures in this regard and has developed a suite of forms to be employed. KMZ Rosenman is also experienced in pursuing wrongdoers who have breached security or otherwise obtained information a company did not intend to become public.

For more information, please contact the following KMZ Rosenman Entertainment and Media attorney:

Susan A. Grode, Partner and Practice Chair  
310.788.4410  
susan.grode@kmzr.com

Research assistance for this Client Advisory provided by Angela Rochester of Northeastern University School of Law.

*Published for clients as a source of information about current developments in the law. The material contained herein is not to be construed as legal advice or opinion.  
© 2002 Katten Muchin Zavis Rosenman. All rights reserved. Katten Muchin Zavis Rosenman is a law partnership including professional corporations.*

## **KMZ Rosenman** KATTEN MUCHIN ZAVIS ROSENMAN

[www.kmzr.com](http://www.kmzr.com)

525 West Monroe Street  
Suite 1600  
Chicago, IL 60661-3693  
Tel 312.902.5200  
Fax 312.902.1061

575 Madison Avenue  
New York, NY 10022-2585  
Tel 212.940.8800  
Fax 212.940.8776

2029 Century Park East  
Suite 2600  
Los Angeles, CA 90067-3012  
Tel 310.788.4400  
Fax 310.788.4471

1025 Thomas Jefferson St., N.W.  
East Lobby, Suite 700  
Washington, DC 20007-5201  
Tel 202.625.3500  
Fax 202.298.7570

401 South Tryon Street  
Suite 2600  
Charlotte, NC 28202-1935  
Tel 704.444.2000  
Fax 704.444.2050

260 Sheridan Avenue  
Suite 450  
Palo Alto, CA 94306-2047  
Tel 650.330.3652  
Fax 650.321.4746

One Gateway Center  
Suite 2600  
Newark, NJ 07102-5397  
Tel 973.645.0572  
Fax 973.645.0573