CYBER PIRATES!

Responding to Internet Theft

By Patrick O'Donnell

A teen working on a school report for his government class turns to the Internet, that lightning-fast and ever-growing repository of every sort of information imaginable. His teacher has advised him to start at U.S. government sites, many of which are quite helpful and relatively authoritative. Being an experienced navigator of cyberspace, he skips the search engines with their dozens of false hits and simply types "whitehouse.com" into his browser.

He's in for an unpleasant surprise. Instead of the presidential seal and press releases about tax cuts at home and spy planes in China, his computer pulls up a cornucopia of sexually explicit images. Shocked, and believing his typo-prone fingers have betrayed him, he quickly (well, relatively quickly) retypes the domain name and hits enter, only to see more of the same. He has stumbled upon cyberpiracy.

Whitehouse.com is the most infamous, but far from the only Internet domain name designed to take advantage of a famous name to which the Web site operators have no connection. The practices generally described as cyberpiracy lack universally accepted definitions, but the main variations are as follows. In classic cyberpiracy, the operator sets up a Web site under a domain name similar to a well-known name to lure surfers looking for the famous name. (The Web site for the White House where Mr. Bush works is at whitehouse.gov.) A closely related practice is cybersquatting in which registrants of domain names based on famous names try to

Patrick O'Donnell is an attorney with the firm of Harris, Wiltshire & Grannis LLP, in Washington, D.C.

sell them to the owners of those names, who can then buy their way out of the potential trouble and embarrassment. And a third, particularly inventive practice is called typosquatting, in which someone registers a name that is just slightly off a famous one. For instance, if you type whitehous.com into your browser, you will be directed to neither Mr. Bush nor nude photographs but to a commercial site called megago.com.

The problem has reached museums and other cultural organizations, too. A Thai law firm reports that the first Thai cyberpiracy case involves a museum focusing on Thai art and architecture called the Jim Thompson House. And last year, the Sydney Opera House won an arbitration against a local computer firm that had registered the name sydneyoperahouse.net. The following is an explanation of the nature of the problem and your museum's legal options for dealing with it.

Background

A basic domain name consists of two parts, the second-level domain name and the top-level domain name. All World Wide Web addresses end in a top-level domain name—the familiar *.com*, *.net*, *.edu*, *.org*, *.gov*, etc. Second-level domain names are the descriptive parts just to the left of the dot, like aam-us in AAM's Web address, www.aam-us.org.

The number and type of top-level domain names are controlled by ICANN—the Internet Corporation for Assigned Names and Numbers—under an agreement with the U.S. Department of Commerce. ICANN accredits registries, which keep master lists of domain names correlated with the numeric codes computers use to find them. Each day a group of core computers, the "root servers" upon which the entire Internet relies, download the master list for each top-level domain name from the appropriate registry, ensuring that any computer using the Internet is guided to the correct Web site.

The registries contract with registrars (not the kind who work in museums) who in turn deal with people who want to buy a domain name. The registrars are primarily middlemen; you ask them if a given name is available, they tell you whether it is, and if so, they register it to you. You give them technical data about your Internet service provider (ISP) and the computer that will host your Web site, which they give to the registry for the appropriate top-level domain. You also give them identifying and contact data about yourself, which they make publicly available in a "whois" service, allowing anyone on the Web to find out who has registered a particular domain name.

The registrars by and large do not screen registrants for *.org*, *.net*, and *.com* names. They do require registrants to click through boilerplate agreements in which they generally promise not to infringe upon a trademark or engage in any other illegitimate use, but do not check into or enforce such clauses.

Legitimate registrants and cyberpirates alike can acquire domain names quickly, cheaply, and nearly anonymously. Some registrars charge as little as $19. With online registration and payment, it's easy to register using false contact information, so victims may have a great deal of trouble locating cyberpirates.

Using an infinite variety of famous names a cyberpirate can obtain many illegitimate domain names. According to press accounts, one Pennsylvania man named John Zuccarini has registered names echoing Oprah Winfrey, Nicole Kidman, Dilbert, Microsoft's Encarta, and Encyclopaedia Britannica, and he has been involved in cyberpiracy suits with other entities ranging from the Dave Matthews Band to The Wall Street Journal.

Changes in the Top-Level Domains

Ongoing additions of the domain-name regime will expand the possibilities for cyberpiracy. ICANN plans to open a new range of top-level domains: *.biz*, *.info*, *.pro*, *.aero*, *.name*, *.coop*, and *.museum*. Network Solutions, Inc. (NSI), the current registry for all *.com*, *.net*, and *.org* names, recently announced a "testbed" program allowing non-Roman characters (Chinese, Korean, Japanese, Arabic, Hebrew) in some of the existing domain names. Both changes add new ways for cyberpirates to capitalize on the famous names of others.

The newly sanctioned top-level name .museum, promises museums some protection against cyberpiracy because the anticipated registrar—the Museum Domain Management Association (which goes by MuseDoma and can be found at www.musedoma.org)—proposes to give *.museum* domain names only to institutions meeting the definitional standard set by the International Council of Museums. MuseDoma also proposes to follow a specified, three-level descriptive naming convention, not the first-come, first-served free-for-all approach that characterizes the *.com* name. Though the procedures for these new *.museum* names had not been finalized at press time (indeed, MuseDoma has yet to finalize the contract authorizing it to embark on this project), they have been under discussion for some time. It seems clear that conflicts over *.museum* names are more likely to involve conflicting legitimate claims to domain names (for example, several museums focusing on black history might seek american.blackhistory.museum) or non-legal disputes over whether the three-level, hierarchical naming convention under consideration is too cumbersome rather than true cyberpiracy disputes.

But the threat of cyberpiracy in the older domain names remains. A *.com* name will often continue to be a Web surfer's first guess; *.com* names may remain popular for museums, just as they are for other entities; and *.com* names (along with *.org* and *.net*) will continue to show up in search-engine results.

What You Can Do

Register Multiple Variations of Your Name

It may be galling, and it may be expensive, but the first and best line of defense against cyberpirates of any flavor is to buy up as many alternate versions of your museum's domain name as you can think of and afford. If your institution has become well-enough known to become a possible target of cyberscams, consider buying your name in every top-level domain open to you: *.org*, *.com*, and *.net*, today, and *.museum*, *.biz*, *.info*, etc., tomorrow. To truly maximize protection, buy not just your proper name but also common short forms, acronyms, and nicknames. And, if you are very well known, consider buying conceivable typos based on your name.

Fees can run into hundreds of dollars annually, but it is