Domain Names, Cybersquatters, and the Law

Who's to Blame?

Shawn M. Clankie

"Must a name mean something?" This is the question that Alice asked Humpty Dumpty in Lewis Carrol's *Through the Looking-Glass* (1872/1963). Humpty Dumpty clearly believed, as many companies do today, that names must have meaning. In cyberspace, this desire for meaningful names, here in the form of domain names or Universal Resource Locators (URLs), has created a fierce battlefield pitting companies against each other, and against speculators, mom-and-pop businesses, foreign firms, and individuals. The race to register every potentially meaningful word or phrase has in turn created a black market for domain names, led by speculators hoping to cash in on the names they have registered. This paper focuses on these speculators, or what have been commonly called cybersquatters.

Cybersquatters are those who have registered domain names, frequently hundreds at a time, with the express intent of either selling them (at a substantial markup) to the highest bidder or of holding the name to prevent others from access to it. Often these registered names will include the trademark

Shawn M. Clankie, Institute of Lanauge and Culture Studies, Hokkaido University, Kita 17, Nishi 8, Kita-ku, Sapporo 060-0817, Japan

of a particular company. The desire of the cybersquatter is to force the company whose trademark has been registered (in URL form) to purchase that domain name from the cybersquatter. With the recent legislation aimed at limiting the abilities of cybersquatters (i.e., the 1995 Trademark Dilution Act), and several court cases favoring businesses over cybersquatters (e.g., *Panavision International v. Toeppen*, 1998, summarized in Manzone, 1998), it is appropriate to question whether all blame should be placed upon individuals alone as cybersquatters. An examination of the registration process will show that existing regulations actually foster cybersquatting, and that not only are individual cybersquatters guilty of this form of crime, but so are corporate cybersquatters.

The Domain Name Game

Domain names, or Universal Resource Locators (URLs), are the addresses that allow consumers, researchers, and others to access a web site. For many years, these domain names were not names at all, but rather purely numeric sequences or IPs (Internet Protocol addresses) identifying the location of an Internet site. Then, a discovery was made. As with telephone numbers, one could produce alphanumeric mnemonic devises out of the sequences. The *1-800-FLOWERS* and *1-800-CALL-ATT*s of the world have given rise to *www.1-800-FLOWERS.com* and *www.att.com*, and the unmemorable purely numeric sequences have been relegated to the underlying role of identification between computers and servers. And that is where the trouble began.

Once the value of the domain name was realized as a mnemonic device and the Internet as a commercial entity (as opposed to being solely the tool of those in education or the government), the boom to register names was underway. At the same time, the registration of domain names was given to the company Network Solutions. The registration process was simple, far easier than the registration of other types of proprietary names (e.g., brand names). To register a domain name one simply had to pay a nominal fee and any name (with limited exceptions) that had not previously been registered could then be obtained. Neither requirements of use nor trademark searches were necessary. The system was nothing more than first-come first-served.

This system was only the first of several problems that would arise and it was not long after registration began that accusations started to fly from companies slow to react to the potential opportunity the Internet provided. Many of these companies found when trying to register their brand or company names that someone else had already registered them. And it is not only commercial businesses that are having this problem, universities too have found themselves facing cybersquatters hoping to cash in on the university's success (Leibowitz, 2000).

Initially the only regulations on registration were that all domain names were to be constrained in terms of length: no more than 26 characters including the dots (Friedman, 1998), category, e.g., commercial entities are followed by .com, educational institutions by .edu, and so forth (Posch, 1998), and location, e.g., .jp for Japan, .fr for France, etc. Yet, the length constraint above creates (albeit unintentionally) a further limitation by creating a finite set of possible domain names. Although there is an enormous number of potential names they are entirely that, potential names. Yet, nearly any name of value, as well as just about every generic commercial entity from *groceries* to *drugs* to *vodka*, has already been registered. And it is not even the entire URL that is required. In most Internet browsers now available one can simply type in the name (exclusive of the www. or .com) and access a site. If one types *ESPN* the browser will automatically take the viewer to the ESPN web site. Companies are well aware of this fact and hence desire to guarantee that their site comes up without any confusion or diversion to another company's site. Similarly, businesses maintain that consumers not knowing the precise URL of a particular company often employ a guessing strategy. In other words, consumers often guess the URL. Therefore, if the desired web site is for *United Airlines*, a consumer may type *United* into the URL line. Companies know that this is how many users search for web sites and they count on it. We must keep in mind here that this creates a further problem in that unlike the real world where it is possible to have *United Airlines* and *United Auto Workers*, in cyberspace there can be only one *www.united.com* and only a single web site accessible when United is typed into the URL line. There are, however, literally hundreds of companies bearing the name *United*. So, who is entitled to the name? In the wild frontier of cyberspace, this has traditionally been decided by the first-come first-served approach, meaning that if the *United Berry Pickers of Maine* registered the name first then every other company must find an alternative. The perceptive reader may suggest that these companies could simply create longer names such as www.unitedairlines.com, and although this is true in some cases, we must keep in mind that most people do not employ the entire name *United Airlines*; rather they simply refer to United (e.g, I fly *United* to Las Vegas). Imagine the problems of registration for names such as *www.apple.com*. Who is entitled to this? It is *Apple Computer* that has registered the name, but is their claim any more legitimate than Washington apple growers or any of the host of other companies or organizations that employ the Apple name?

Who Owns the Name?

Now that we have established the inherent difficulty in the distribution of domain names, we can turn to the question of who owns the name. As a

linguist, my initial reaction would be that no one owns any name. At best we are temporary caretakers of a name. I cannot stop others from naming their children *Shawn* for example. If we withdraw the association of the company to its brand name we are simply left with lexical items, and as such they are available for use by any user of the language as with any other word of the language. But in the business and legal arenas, the issues are not quite that simple. Proprietary law has granted *limited* protection to those who register a brand name or other form of trademark and, at present, domain names are being treated in a similar way to that of the brand name (see, for example, *Playboy Entertainment v. Frena*, 1993). The key word here is *limited*. The laws protect one company from infringement on the name by another company but it cannot prevent, for example, use of the name in speech by an individual, or in other areas such as parody. In other words, the law protects the holder of the name from *commercial infringement*, and to a lesser extent *dilution*, or weakening through unauthorized use by others. For example, *www.candyland.com*, an Internet porn site was found to have diluted the value of the name of the Hasbro-owned *Candyland* game (*Hasbro, Inc. v. Internet Entertainment Group, Ltd.*, 1996). This protection, however, does not give the owner copyright to restrict others from using the name in noncommercial affairs. This limited protection stems back to a 1923 Supreme Court decision (*Prestonettes, Inc., v. Coty*) that initially granted proprietary right to the name. In that court case, Justice Holmes wrote,

> Then what new rights does the trademark confer? It does not confer the right to prohibit the use of the word or words. It is not copyright.... A trademark only gives the right to prohibit the use of it so far as to protect the owner's good-will against the sale of another's product as his.... When the mark is used in the way that does not deceive the public, we see no such sanctity in the word as to prevent its being used to tell the truth. It is not taboo. (In Schecter, 1925, p. 155)

Companies, however, frequently believe that they hold absolute right to the name, even if they themselves have pilfered the name from the vernacular language. We need to look no further than attempts of companies and the International Trademark Association (INTA) to restrict the generic use of brand names by lexicographers producing dictionaries (Clankie, 1999b, Landau, 1994, p. 395). In 1999, the automobile maker *Porsche* filed suit against 135 entities employing the Porsche name, or a variation of that name in their URLs (CNNfn, 1999). Hughes (1988) characterized the view of language in the eyes of the business community thus:

> Linguistically, all modes of advertising now assume that the language is simply a resource, to be appropriated, abused, plundered or modified for any marketing purpose. This attitude to language derives from the profit motive, from anonymity and from the mass scale of advertising campaigns. (p. 155)

The question that should now be raised is whether the companies themselves engage in cybersquatting. A common practice at many companies at present is to purchase their trademarks in the form of a URL, as well as common misspellings of their name (for which they may or may not possess the trademark). They do so to maximize their chances of a consumer entering their site. Although this may seem to be good business practice, it too limits others from accessing available names. By purchasing all approximation of the trademark, companies can effectively limit anyone from purchasing similar names. Is this not a form of cybersquatting? What if a family business in Illinois named *Appel*, a business that may have been selling its product for a century or more under the family name then desired to register its name for use on the Internet? If, for example, *Apple Computer* had bought the *Appel* name with the sole intent to secure additional viewers who had misspelled the Apple Computer URL, the Appel family business would not be permitted to use the name as a domain name, even though Apple Computer would have no intention of using *Appel* for anything more than a link, and even though there is no other similarity between the two firms. Further blurring the lines, companies engaging in this practice then police not only for other URLs using the trademark but also any popular misspellings of the name they may or may not hold rights to (see for example, Nelson, 1998, p. 6), and any names that may sound phonetically similar. They then send out cease and desist orders against holders of the URLs too similar to the trademark. Continuing on with our hypothetical Appel/Apple example, holders of the *www.epple.com*, *www.aepl.com*, etc. could find their names being challenged simply for "sounding" too much like the Apple Computer URL.

A further yet more devious way of engaging in this form of corporate warfare involves companies that go so far as to buy up the potential domain names of any competitors. For example, *Princeton Review, Inc.*, bought the domain name *www.kaplan.com*, the name of its prime rival to limit its access to a successful name (Gole, 1999, p. 403). Again one must ask, are companies not guilty of the same tactics employed by individual cybersquatters?

Cybersquatting as an Internet Crime

At this point it should be apparent that the newness of the system and the practice of first-come first-served have resulted in a number of difficulties and that the problems of domain name availability cannot be placed solely upon individuals as cybersquatters. Yet, it is the individuals who are often the first to be blamed when a name is unavailable. In this section it will be important to consider whether cybersquatting is indeed a crime.

If we first consider the nature of cybersquatting, the intent of the

cybersquatter is to hold hostage the name until a buyer pays a suitable price or alternatively to prevent others from using the name. Not all individuals who buy up blocks of names, however, can be considered cybersquatters. To fully understand this we must turn once again to the registration process. It is the names that are already registered trademarks that are of the most concern. Not all names, however, can be seen to fit into this system. Under current trademark law, domain names are being treated in this way; generic words, those general nouns like *ice*, *plants*, and *food*, are not normally registerable as trademarks for companies with an inherent relationship to the generic form. For example, *Hershey's* would not be able to register the proposed brand name *chocolate* as a trademark because it is the generic term for the semantic class to which Hershey belongs. However, a company with no inherent relationship could. This is how *Apple* was registered as the brand and company name for the computer maker. Since no one holds any proprietary right to many of these forms, the first-come first-served system works quite well, and the market for such names from seller to buyer should be what the market will bear. If however, the law is to treat domain names like brand names and other forms of trademark, then just as with brand names, such generic registrations would be prohibited in many cases.

Most cybersquatting is generally thought of in terms of the withholding of names with the intent of financially profiting from companies desperate to hold their own names. However, there are also cases of one company purchasing the names of its competitors with the intent of limiting access to the Internet marketplace. Most often this type of cybersquatting is done by businesses.

One further concern is a new type of cybersquatting. This form involves companies and speculators buying every available surname with the intent of profiting from people wishing to set up their own web sites or web email addresses. One company *Mailbank.com* hold 14000 surnames, covering 60% of the U.S. population (Woolley, 1999, p. 244). Should companies with no inherent interest in these names be permitted to sell them back to the consumer willing to pay the highest price for his or her own name? There is something unethical about this practice. Personal names are perhaps the most sacred of all names we have in English and turning them into a commodity takes business ethics to a new low.

Is cybersquatting a crime, the answer is clearly yes. Yet, cybersquatting and the laws regarding cybersquatting must be clearly defined. If domain names are to be governed under existing trademark law, then the same registration process involved in brand name registration should apply to domain names. If they are to be treated differently, then applying a preconceived set of laws to an entity that is different is destined to fail. New laws will be required. Rather than creating laws to deal with cybersquatters, however, both companies and individuals would be better served by a registration process that requires both a trade-

mark search and actual usage (the site must be put to use within a given period or the URL will be forfeited). This is beginning to happen.

Similarly, registration of a generic name for a product within the same semantic class (as in the Hershey's example above) would need to be forbidden, just as it is with brand names. Yet, from the current trend in legislation (e.g., The "Anti-cybersquatting Consumer Protection Act" proposed in 1999 by Senator Orrin Hatch), the government continues to insist that cybersquatters are the problem. Fines of up to $300,000 for cybersquatting have been brought into law (Leibowitz, 2000). Ironically, the use of the phrase "consumer protection" in the title of The Anti-Cybersquatting Consumer Protection Act is a slap in the face to consumers. The bill has little to do with consumer protection, unless the consumers they refer to are the trademark holders. Yes, cybersquatting is a crime. But cybersquatting is also an effect, the cause of which lies squarely with the government.

Conclusions

The common perception of the cybersquatter as a single individual buying up hundreds of names only to sell them back to companies, at best, ignores the full extent of the problem. It is true that many individuals are trying to cash in on the Internet, but there are many companies that in turn are taking advantage of the same loopholes in the registration process that the law affords. Cybersquatting is a crime. To hold hostage a name for profit is extortion. To restrict others from legitimately using the name is censorship. But to blame individuals alone, without considering the inherent fault in existing regulations and the role of companies as corporate cybersquatters is like pulling the body of a tick away from one's skin only to leave the head behind. To answer the question posed in the title of this article, *Who's to blame?*, we must first lay blame at the hands of the government for permitting a system that allows anyone to register any name through the haphazardness of the first-come first-served system. This has allowed cybersquatting to take place. The band-aid solution of applying current trademark law to cybersquatters without applying the same law to the registration process that permitted them to cybersquat on the names in the first place is irresponsible planning. Similarly, blame must be extended to corporate entities involved in this form of intellectual sabotage as well. Guilt extends to all sides. Only a reproach of the current registration system to bring it more closely in line with existing trademark law can begin to solve the problems of cybersquatting. Attempts such as that of Orrin Hatch are attacking a symptom, but a fuller examination of the causes of cybersquatting within the current system is needed. Until that is achieved, cybersquatting will continue, at a considerable expense to legitimate users of the name.

References

Carrol, L. (1963). *Through the looking-glass.* New York: MacMillan.

Clankie, S. (1999a). On brand name change: A theory of genericization. (Doctoral dissertation, University of Hawai'i at Manoa). *Dissertation abstracts international, 60(8)*, #9940612.

Clankie, S. (1999b). Generic brand name change in creative writing: Genericide or language right? In L. Buranen and A. Roy (Eds.), *Perspectives on Plagiarism and Intellectual Property in a Post-Modern World* (pp. 253–262). Albany, NY: State University of New York Press.

Federal Trademark Dilution Act. 15 U.S.C. §§ 1125(c), 1127 (1995).

Friedman, J. (1998). How to protect your Web site's name: In's and out's of Internet domain names. *Folio: The Magazine for Magazine Management, 27(1)*, S236–237.

Gole, R. (1999). Playing the name game: a glimpse at the future of the Internet domain name system. Federal *Communications Law Journal, 51(2)*, 403.

Hatch, O. (1999). *Markup of S. 1255, the anticybersquatting consumer protection act.* [On-line], Available: http://www.senate.gov/~hatch/state101.html.

Hasbro, Inc. v. Internet Entertainment Group, Ltd., No. C96-130WD, 1996 WL 84853 (W.D. Wash. 1996).

Landau, S. (1994). *Dictionaries: The art and craft of lexicography* (2nd ed.). New York: Charles Scribner's Sons.

Leibowitz, W. (2000, Jan. 21). As "Cybersquatters" multiply, colleges try to protect their good names. *The Chronicle of Higher Education*, A39ff.

Manzone, U. (1998). Trademark: domain name-dilution. *Berkeley Technology Law Journal, 13(1)*, 249–264.

Nelson, M. (1998, June 22). Service providers up in arms over misspelled domain names. *InfoWorld, 20(25)*, 6.

Panavision International v. Toeppen (1998). 9Th Circuit Court #97-55467.

Playboy Entertainment v. Frena (1993). 839 F. Supp. 1552, 1559–1560.

Porsche "cybersquatter" suit to start Friday. (1999, May 27). [On-line], Available: http://cnn.com/digitaljam/newsbytes/131274.html.

Posch, Robert, Jr. (1998). Trademark protection for Internet domain names. *Direct Marketing*, 61(3), 63-64.

Prestonettes, Inc., v. Coty (1923). 264 U.S. 359, 368.

Schecter, F. (1925). *The historical foundations of the law regarding trade-marks.* New York: Columbia University Press.

Woolley, S. (1999, July 26). Master of your domain. *Forbes*, 244.

About the Contributors

Shawn M. Clankie is a frequent writer on issues of names and the law. In 1999, he received a Ph.D. in Linguistics from the University of Hawai'i at Mānoa. His dissertation research presented a theory to account for generic change in brand names. He is currently on the faculty of the Institute of Language and Culture Studies at Hokkaido University in Sapporo, Japan.

Edward Cline is an independent scholar and novelist.

Russell Eisenman, Ph.D., is a faculty member at the University of Texas and a prolific author.

P. N. Grabosky, Ph.D., is Director of Research at the Australian Institute of Criminology.

Anthony J. Graybosch is professor of philosophy at California State University–Chico. His areas of interest are American philosophy, ethics and the family, and rock and blues.

Robert Hauptman edits the *Journal of Information Ethics*.

Jack Hibbard, Ph.D., is a faculty member at St. Cloud State University.

Steve McKinzie is currently the Social Science Liaison Librarian at Dickinson College, Carlisle, Pennsylvania. McKinzie tries to review and write for the library field as much as he can, believing that librarians generally are not as controversial or polemical as they ought to be.

Russell G. Smith, Ph.D., is senior research analyst at the Australian Institute of Criminology.

Cassandra Van Buren, Ph.D., is an assistant professor in the Communication Department at Trinity University in San Antonio, Texas. Her research and teaching center on communication, technology, and culture.