

# ALSTON & BIRD LLP

The Atlantic Building  
950 F Street, NW  
Washington, DC 20004-1404

202-239-3300  
Fax: 202-654-4839  
www.alston.com

Eric Shimp, Policy Advisor

Direct Dial: 202-239-3409

Email: eric.shimp@alston.com

May 9, 2013

VIA EMAIL

Douglas Bell  
Chair, Trade Policy Staff Committee  
Office of the United States Trade  
Representative  
Washington, DC

Re: **Transatlantic Trade and Investment Partnership**  
**Docket: USTR-2013-0019**

Dear Mr. Bell:

I am writing on behalf of the Coalition Against Domain Name Abuse, Inc. (CADNA), a 501(c)(6) not-for-profit corporation founded in 2007. CADNA seeks to make the Internet a safer and less confusing place for consumers and businesses alike. Its mission is to decrease instances of cybersquatting in all its forms by facilitating dialogue, effecting change, and spurring action on the part of policymakers in the national and international arenas.

CADNA is dedicated to building awareness about and advocating action to stop illegal and unethical infringement of brands/trademarks online. Taking action against the practices of cybersquatting, CADNA provides a framework for brand owners to protect themselves—as well as their investors, customers and partners—from illegal trademark infringement.

CADNA's 16 member organizations include US and European-based corporations who represent a cross-section of global brand leaders. Our members share recognition in the critical importance of protecting brands, trademarks and consumers online.

## **Cybersquatting: Online Piracy and Domain Name Trademark Infringement**

Cybersquatting is the bad-faith registration of a domain name that includes or is confusingly similar to another party's trademark. Cybersquatting has evolved over the

past decade into a sophisticated form of online piracy that now costs US industry in excess of \$1 billion annually, while exposing consumers to fraud, identity theft and possibly harmful counterfeit products. Industry suffers losses result from diverted traffic, the loss of consumer trust, and increased expenses of protecting consumers from Internet-based fraud. Revenues lost to cybersquatting may not be invested in company expansion, new hires, or capital expenditures, a negative multiplier effect in the current economy.

By using domain names to exploit the trust that consumers have in legitimate brands and trademarks, cybersquatters are able to harm consumers through spam, spyware, malware, phishing, and the sale of unwanted counterfeit goods. The magnitude of the problem is great. The overall number of domain names has more than doubled since 2003, and the growth of cybersquatting has exceeded that pace. According to a recent independent report, cybersquatting increased by over 200% in 2007 vs. 2006 alone.

### **The Economic Impact on Brandowners and Consumers**

According to research conducted by CADNA in conjunction with the domain and market research consulting firm FairWinds Partners, the economic impact of cybersquatting is significant:

- The practice costs brand owners worldwide over \$1 billion U.S. dollars every year as a result of diverted traffic, the loss of hard-earned trust and goodwill, and the increasing enforcement expense of protecting consumers from Internet-based fraud.
- Depending on the brand owner's industry, the total impact of cybersquatting on a single brand could be tens of millions of U.S. dollars when factoring in the value of lost leads and sales, costs of brand dilution, consumer confusion, poor customer experiences and millions of lost unique visitor impressions each week.
- Excluding less-tangible costs such as lost goodwill and poor customer impressions, the impact of cybersquatting on trademark holders is in excess of \$1 million per brand, per year. Some well-known brand owners will face losses many times this figure.
- Direct financial damages to consumers through cybersquatting is difficult to quantify. Cybersquatting, however, remains a primary vehicle for delivery of spam and phishing attacks, and as the means by which malware and spyware are deposited on consumers' computer systems worldwide. A 2007 study by the ITU reported estimated damages from malware, spyware and phishing to be \$7.1 billion to US consumers in the year 2006.

## **Existing Legal Frameworks Offer Insufficient Protection to Consumers and Trademarks**

The U.S Congress was the first national legislature to recognize cybersquatting as a new form of online piracy. Congress enacted the Anti-Cybersquatting Consumer Protection Act (ACPA) in 1999 as an initial means for brand owners to seek redress against cybersquatters. Today, however, the Internet is a very different place than when ACPA was originally drafted into law. Cybersquatters are no longer dependent on domain name sales for profit. Automated programs acquire domain names and establish pay-per-click sites with minimal human involvement, allowing this form of piracy to take place on a massively expanded scale. As a result, it is possible for operators to control and monetize hundreds of thousands, or even millions, of Internet domain names.

In the United States, the provisions offered by the ACPA have been overwhelmed by the volume and sophistication of contemporary online piracy. Other national jurisdictions lack even the foundational legal protections provided by ACPA. Internationally, trademark owners have little recourse other than the domain name dispute resolution process provided by the WIPO Arbitration and Mediation Center. These remedies neither deter nor slow the pace of domain name piracy. Trade agreements, whether bilateral or multilateral in nature, have also failed thus far to address cybersquatting and domain name abuse as infringements of intellectual property rights. Consumers, meanwhile, have virtually no legal tools with which to defend themselves against this form of online crime.

## **Internet Governance: new gTLDs Deliver More Risk, Stir Congressional Interest**

The Internet Corporation for Assigned Names and Numbers (ICANN) coordinates many functions of the Internet globally, including the Domain Name System and the generic (gTLD) and country code (ccTLD) Top Level Domain systems. ICANN's recent initiative to expand the number of gTLDs exacerbates the risk of cybersquatting and domain name abuse to brand-owners and consumers alike.

To date, the number of gTLDs, such as ".com" and ".org", total 22. In 2013, however, the Internet community could begin to see what will be upward of 1,000 new gTLDs. During the application period, the Internet Corporation for Assigned Names and Numbers (ICANN) received in excess of 1,900 applications for new gTLDs.

Trademark owners and pro-consumer non-profits alike are highly concerned over the attendant proliferation of cybersquatting and domain name piracy that is certain to stem from the 550 of those gTLDs that will be open for public registration, much like .com.

The US Congress, too, has taken an active role over the past year in seeking to slow ICANN's pursuit of expanded domain names and to ensure greater protections for

trademarks and consumers in the new Internet environment. The topic was the subject of multiple Congressional hearings in late 2011.

ICANN's handling of the gTLD rollout process has done little to reassure US legislators or the US business community. In August 2012, Senate Judiciary Chairman Patrick Leahy (D-VT) and Ranking Member Charles Grassley (R-IA), joined by House Judiciary Chairman Lamar Smith (R-TX) and Ranking Member John Conyers (D-MI) sent a joint letter to ICANN requesting information regarding the organizations efforts to protect trademark owners from cybersquatting and raising question's regarding ICANN's treatment of public comments critical of the new gTLD program.

The global impact of the new universe of gTLDs promises to have a significant impact on trademark security, as well as the preservation of the Internet as a secure, trusted environment for consumers.

### **The Transatlantic Trade and Investment Partnership: Potential Action**

CADNA believes the United States and European Union have the opportunity to take joint regulatory steps in the TTIP to address the issue of cybersquatting and domain name abuse. Consumers in the United States and Europe alike fall prey to cybersquatting and its associated ills on a daily basis. Trademark owners in both the US and EU, of which CADNA's membership is representative, are seeking cooperative regulation aimed at setting high, global standards for online protections of trademarked domain names.

Any actions undertaken by the United States and European Union on domain names will take place within the context of an ongoing global discussion regarding Internet governance. CADNA supports the multi-stakeholder model of Internet governance, and the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN is not perfect and there remains much work to be done to improve its transparency and accountability, but CADNA fundamentally supports ICANN's mission and role in overseeing the Domain Name System (DNS).

U.S. government policy also supports the multi-stakeholder system. As he noted in remarks February 28th, 2012, before the GMSA Mobile World Congress in Spain, Robert M. McDowell, Commissioner of the Federal Communications Commission, rightly observed that "modification of the multi- stakeholder Internet governance model may be necessary...but we should all work together to ensure no intergovernmental regulatory overlays are placed into this sphere." Commissioner McDowell continued to say that, "not only would nations surrender some of their national sovereignty in such a pursuit, they would suffocate their own economies as well, while politically paralyzing engineering and business decisions within a global regulatory body."

Governments, ICANN, and industries all have a role to play in the global advancement of Internet policies that protect and promote their companies and consumers, and it is in their proper coordination that the Internet will be a safe and

flourishing place for Internet users. CADNA believes that national governments have a role to play in establishing coordinated national laws and policies to serve as effective deterrents to cybersquatting and domain name abuse.

National laws and policies on both sides of the Atlantic should serve as effective deterrents to cybersquatting and domain name abuse. CADNA recommends the US and EU develop potential regulatory changes to accomplish this objective, through both the Intellectual Property and Regulatory Cooperation provisions to be negotiated in the TTIP. Reforms should address the following areas:

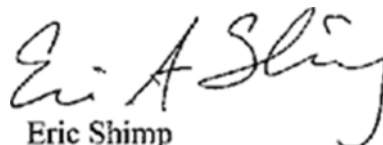
- Mandate responsibility through the Internet service supply chain. Current regulation allows cybersquatters to obtain domain names for illicit use through third-party service providers who are free from liability. These service providers, (registrars, agents and/or representatives), and in some cases Internet Service Providers themselves, in turn profit from revenue-sharing arrangements with cybersquatting entities through Internet landing pads, parking spaces, pay-per-click advertising and monetization reports. Laws should eliminate this shelter for cybersquatters, and expose all who knowingly profit from the illicit activity to liability.
- Establish liability against agents, representatives, or any other persons or entities in active concert or participation with cybersquatters and derive profit from such illicit activities.
- Establish more inclusive jurisdiction. Unfortunately, the global nature of the Internet means that, like cybersquatters themselves, domain name registrants, agents, representatives, registrars and registries may exist outside U.S. or European Union territory, but still facilitate and profit from online piracy. An ideal course of action would restrict the ability of cybersquatters to access U.S. and EU consumers.
- Expand plaintiffs' access to civil remedies. Trademark owners and consumers alike should be furnished the opportunity under national laws to bring civil actions against domain name registrants and their agents or representatives throughout US and EU jurisdictions.
- Foster deterrence through statutory damages. Under current U.S. law, cybersquatters face statutory damages of between \$1,000 and \$100,000 per domain name. The courts have, however, generally awarded limited damages closer to \$1,000 per domain name. For brand-owners, the cost of filing and pursuing legal action far exceed the potential damages the mark owner is likely to be awarded. For consumers, such ineffective enforcement leads to greatly expanded risk in the course of regular Internet use.
- Create damage provisions in relevant national laws to create an effective deterrent against cybersquatters, When an entity has been found to engage in widespread commercial scale cybersquatting, the presumption should be that damages start at the

higher end of the scale and can be lowered at the court's discretion. Damages per violation should have a floor of \$25,000.

- Create an information clearinghouse for US and EU consumers regarding malafide domain names and registrants and registrars associated with them.

On behalf of CADNA and its member organizations, we thank you for your consideration of our comments as the US Government develops negotiating positions for the Transatlantic Trade and Investment Partnership. Our organization and corporate members are prepared to work with both governments to ensure the TTIP includes appropriate protections for brands on the Internet, safeguards the consumer experience online, and addresses cross-cutting issues of Internet governance which impact free market competition, innovative intellectual property, and consumer choice and safety.

Sincerely,



Eric Shimp  
Policy Advisor

#### **CADNA Member Organizations**

- American International Group, Inc.
- Bacardi & Company Limited
- Carlson / Carlson Hotels / Carlson Restaurants
- Dell Inc.
- DIRECTV, Inc.
- Eli Lilly and Company
- Harrah's Entertainment, Inc.
- Hewlett-Packard Company
- Hilton Worldwide, Inc.
- LEGO Juris A/S
- Marriott International, Inc.
- Morgan Stanley
- Nationwide Mutual Insurance Company
- New York Life Insurance Company
- Wells Fargo & Company
- Wyndham Worldwide Corporation