



Testimony of Josh Bourne
President and Co-Founder
Coalition Against Domain Name Abuse
Before the Committee on Homeland Security and Governmental Affairs
Hearing on Cyber Attacks: Protecting Industry Against Growing Threats
September 14, 2009

Mr. Chairman and distinguished members of the committee, thank you for convening this timely hearing on issues concerning cybersecurity. Today, there are over 1.5 billion users of the Internet, but it is likely that less than one percent of the users are even aware that Internet policy is set by the Internet Corporation for Assigned Names and Numbers (ICANN), let alone how the drastic changes ICANN is about to implement will dramatically impact the space. Given the commercial significance of the Internet and the potential national security threats possible through the Internet, it is critical that the United States Congress involve itself in matters of domain name space policy and regulation.

My name is Josh Bourne and I am the president and founder of the Coalition Against Domain Name Abuse (CADNA). CADNA, a 501(c)(6) non-profit association, was founded over two years ago with the help of Fairwinds Partners and leading brand owners to combat a variety of abuses on the Internet. CADNA represents businesses vital to the American and global economies, including American International Group, Inc., Bacardi & Company Limited, Carlson/Carlson Hotels Worldwide/Carlson Restaurants Worldwide, Compagnie Financière Richemont SA, Dell Inc., DIRECTV, Inc., Eli Lilly and Company, Goldman, Sachs & Co., Harrah's Entertainment, Inc., Hewlett-Packard Company, Hilton Hotels Corporation, HSBC Holdings Plc, InterContinental Hotels Group, Marriott International, Inc., New York Life Insurance Company, Nike, Inc., Verizon Communications, Inc., Wells Fargo & Company, and Wyndham Worldwide Corporation.

CADNA was founded in response to the growing international problem of cybersquatting, which is the bad faith registration of a domain name that includes or is confusingly similar to an existing trademark. Because attracting Web traffic is vital to success in the online space, the loss of users due to negative impressions may bear significant consequences for a company. In addition to the mounting legal costs that companies now face in defense of their own domains, this infringement costs organizations billions of dollars in lost or misdirected revenue. Furthermore, cybersquatting harms Internet users by creating confusion; infringing domains that



potential customers happen upon could be set up by cybersquatters to deposit spyware or malware or host phishing schemes. According to a survey conducted by Gartner, Inc., the average phishing victim in the United States lost \$866 in 2007, with total losses from phishing attacks soaring to \$3.2 billion. Infringing sites could also be set up to intercept emails meant for the proper brand owner, which could contain sensitive information.

CADNA works 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 also aims to build awareness about illegal and unethical infringement of brands and trademarks online.

CADNA seeks to make the Internet a safer and less confusing place for consumers and businesses alike. 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.

Thank you very much for the opportunity to present the views of our organization on this very important topic.

With the Joint Project Agreement (JPA) set to expire on September 30 and reports of a possible new agreement being negotiated to take its place, we feel that it is critical for the Internet community and the US government to pause, take a step back, and reassess the success of ICANN, the not-for profit organization that has day-to-day responsibility for establishing policies and managing the operations of the Internet's domain name system (DNS). ICANN's policies have produced an online environment favorable for cybersquatting, fraud and other nefarious activities.

ICANN is failing to address numerous issues corrupting the Internet: ICANN often ignores issues regarding the safety and stability of the Internet, such as the proliferation of cybersquatting, which can enable phishing, malware deposit schemes, and the sale of unwanted counterfeits. ICANN has also largely ignored the problem of inaccurate WHOIS information, which encumbers the identification and prosecution of bad actors. Rather than helping to make the Web more secure, ICANN is increasing the online risks that businesses and consumers face by irresponsibly releasing new generic top-level domains (gTLDs).

When US policy was developed in the late 1990s, the United States Government thought that by September of 2009 ICANN would exist as a transparent and reliable force for sensible and practical policies for the Internet. Unfortunately, this has proven not to be the case, and so governments must rethink its stance towards ICANN in a thoughtful and considered manner.



Members of the global business community believe that while ICANN has achieved many things, broad participation and involvement of its diverse stakeholders is not one of them. To date, those involved in ICANN policy have not represented the needs of users and user groups that utilize and depend on the Internet in widely varying respects. There is a lack of diversity, cross-constituency interaction, and overall balanced debate and discussion present in ICANN's day-to-day policy development and in international meetings, leaving much to be desired. For example, ICANN recently adjusted the voting structure of its policy-making body, the Generic Names Supporting Organization (GNSO), so that those with financial interests have a majority of the vote rather than allowing all Internet-using constituencies equal participation. While Internet users, businesses, and governments have slowly begun to take a greater interest in the domain name space, we fear that ICANN's current framework does not offer adequate opportunities or incentives to encourage broader involvement. It also does not allow for the development and implementation of good policy.

Unfortunately, ICANN has often fallen short of its duty to maintain the stability, reliability, and security of the Internet and tends to favor certain special interests rather than looking out for the diverse interests of the global Internet community. One prime example of this is the decision to open up the Internet to the creation of a limitless number of extensions, which benefits the very entities that control the GNSO- registrars and registries. Registrars and registries have long been working through ICANN to create policy to regulate the very product that they sell; it is no wonder now that they are pushing for a policy that will give them an unlimited supply of their product, regardless of that product's impact on the market.

CADNA does not claim that there should never again be another gTLD launch; it may very well be true that a new gTLD can provide innovation to the domain name space. However, opening up the floodgates to a potentially unlimited number of gTLDs, with many of ICANN's own staff uncertain about the scalability of operations and with the current domain name space plagued with problems, is dangerous and irresponsible.

ICANN's plans to dramatically increase the number of website names available for registration will make the web exponentially more complex. Given the state of the current domain name governance system, priority should be given to correcting existing issues rather than expanding the space. For example, it is still too easy for cybersquatters to register domain names in bad faith that are lawfully associated with legitimate entities. Even without these proposed gTLDs, cybersquatting grew by 18% in the last quarter of 2008.

Cybersquatters are also extremely difficult to apprehend as a result of ineffectual ICANN



policies. ICANN is aware of the fact that its requirements regarding WHOIS information are weak, leading to faulty or inaccurate information about the identities of cybersquatting domain name owners, but it has yet to adjust its policies. New gTLDs would only exasperate this problem. Rather than allowing this issue to go unchecked, ICANN should resolve it before increasing the size of the domain name space and the opportunities to practice fraud.

Conservative estimates put the average cost per sunrise registration around \$300. If a typical company registered 20 domains in each sunrise period, the cost to participate in all 200 new gTLDs that could be added in 2010 would be \$1.2MM. The costs of participating in new gTLD launches can be much greater than outlined above due to offers of special registrar queues to raise probability of successfully registering a domain, extra validation services, and gimmicky programs presented by new registries. Furthermore, as with gTLDs such as dot-MOBI, dot-EU and dot-ASIA, companies may feel compelled to defensively register hundreds of domains rather than a mere 20.

If brand owners chose to participate in just 10% of the new gTLDs to be launched in 2010, the average expenditure per brand just for 20 trademark sunrise registrations in each could be \$120,000. This represents a steep 37.5 per cent cost increase since the average company spends less than \$200,000/year maintaining their domain portfolio.

Brand owners who are already under water due to infringements in the 1000+ worldwide domain extensions will be forced to contend with the added complexity of policing the use of their brands in domain names. The costs of monitoring and enforcing the new gTLDs are likely to be significant. This is not to mention the brand dilution, proliferation of cybercrime and damage to the integrity of the Internet that are sure to occur. These new gTLDs will afford the most benefit to domain industry insiders, criminals and others that look to profit in an expanded Internet real estate market.

Below is a simple summary of the cost to businesses and consumers that a proliferation of gTLDs will create:

- An average company will spend \$40,000 per year for online and domain monitoring
- Cybersquatting will grow at a rate of 100% year after year
- On average, a global corporation will face 5,000 infringements every year
- 50% of all cybersquatting sites receive meaningful traffic
- Cybersquatting sites that garner meaningful traffic receive an average of 600 visitors/year
- 25% of visitors to Pay-Per-Click (PPC) sites click on the posted links



- Of those who click on PPC sites, 75% click on the link provided and paid for by the brand owner represented in the domain name
- Average cost per click is \$.50 (conservative est. since clicks can be 10+ times this amount)
- An average company files 10 Uniform Dispute Resolution Policy (UDRP) complaints per year (one domain per UDRP)
- The average total cost of each UDRP is \$5,000
- An average company sends 150 cease and desist letters annually (assuming a 100% success rate)
- Cost per cease and desist letter is \$50 (even if generated in-house)

*These estimates do not include an estimate regarding the loss of sales or damage to brand value that occur as a result of cybersquatting activities.

It is important to remember that the average Internet user—every individual that uses the Internet for personal or business use—is also a victim of the current space. As a result of ICANN’s policies, there is a lack of transparency, accountability, and security online, so as Internet users continue to be vulnerable to phishing, malware deposits, diversion, and confusion there remains little opportunity for recourse and retribution. This would only expand exponentially along with any gTLDs that would be added.

Thank you for your time and consideration on this very important matter.

Sincerely yours,

A handwritten signature in black ink, appearing to be "JB" or similar initials, written in a cursive style.

Josh Bourne
President, Coalition Against Domain Name Abuse