



**Before The United States House of Representatives
Committee On The Judiciary**

**Subcommittee on Intellectual Property,
Competition and the Internet**

**Hearing on
“Promoting Investment and
Protecting Commerce Online:
Legitimate Sites v. Parasites, Part II”**

**Statement of Christine N. Jones,
Executive Vice-President, General Counsel,
& Corporate Secretary
The Go Daddy Group, Inc.**

April 6, 2011

Introduction

Good morning, Chairman Goodlatte, and thank you for the honor of speaking before you today on the critical issue of combating illegal and nefarious activity on the Internet. I would also like to extend my thanks and appreciation to Ranking Member Watt, Chairman Smith, and Ranking Member Conyers, as well as the other Members of the Committee, for all your efforts in addressing this important issue.

The Go Daddy Group devotes considerable time and resources to working with law enforcement to preserve the integrity and safety of the Internet by quickly closing down websites and domain names engaged in illegal activities. A vast number of our customers earn their livelihood from the successful businesses they have been able to establish and grow online, and their ability to continue to do so is of paramount importance to us. Go Daddy is committed to doing everything it can to ensure that the Internet is a safe and trustworthy way to communicate and conduct business. We challenge our counterparts on the Internet to make the same commitment.

Background

The Go Daddy Group, Inc. consists of eight ICANN-accredited domain name registrars, including GoDaddy.com. Go Daddy currently has over 47 million domain names under management, and is the number one domain name registrar in the world. In fact, we register domain names at a rate of more than one per second. We are also the world's largest website hosting provider – we currently provide hosting services for more than 5 million websites. Our 50+ additional products and services, including SSL certificates, website builders, and online business tools, are all focused toward helping our customers establish a trusted presence on the Internet.

A domain name registrar serves as the point of entry to the Internet. For example, if you wanted to register the domain name www.ChairmanGoodlatte.com, you could go to www.GoDaddy.com to register that domain name. A domain name registrar is different from a traditional ISP, such as AOL, MSN, or EarthLink. The ISP provides *access* to the

Internet whereas the registrar provides the *registration* service for .com names and the like. In short, in exchange for a fee, the ISP provides the means by which an Internet user connects to the Internet via a dial-up connection, cable modem, DSL, or other connection method. A registrar, on the other hand, enables Internet users to establish a web presence by registering a unique name such as www.ChairmanGoodlatte.com.

A domain name registrar also differs from a domain name registry, in that the registry acts as the database of all domain names that are registered for a particular top-level domain, or “TLD.” TLDs are the suffix that appears to the right of the “dot” in a particular domain name – in www.ChairmanGoodlatte.com, the TLD is “.com.” There are dozens of registries that have received authorization from ICANN to offer particular TLDs, such as .com, .net, .biz, .info, etc. Registrars such as Go Daddy enter into agreements with the various registries to offer the TLDs that are managed by those registries.

Once www.ChairmanGoodlatte.com is registered, you might decide that you want to direct your domain name to a website that contains content, such as items for sale, a blog, news articles, or the like. In order to create and maintain a website on which to store your content, you would need to find a place to store, or “host,” that website. Again, you could go to www.GoDaddy.com for content storage, or hosting, services. A hosting provider differs from a traditional ISP in that the hosting provider supplies space on a computer server that is accessible from the Internet, rather than access to the server, which is provided by the ISP.

How Go Daddy Works To Combat Illegal Activity On The Internet

Go Daddy has made it a high priority to use its position as the world’s largest registrar and hosting provider to make the Internet a better and safer place. As such, we have a large 24/7 Abuse Department whose mission is to preserve the integrity and safety of Go Daddy’s network by investigating and shutting down websites and domain names engaged in illegal activities. We work with law enforcement agencies at all levels and routinely assist in a wide variety of criminal and civil investigations. We are also quick

to respond to public complaints of spam, phishing, pharming, and online fraud, and work closely with anti-fraud and security groups such as the Anti-Phishing Working Group, Digital Phish Net, the National Center for Missing and Exploited Children, and CyberTipLine. We take each instance of illegal activity very seriously and devote high priority to ensuring that websites containing any kind of illegal content – so-called “ParaSites” -- are removed from our network.

As recent examples of our enforcement and takedown activities, we worked with the United Kingdom’s Metropolitan Police Service to shut down or redirect nearly 200 domain names and websites used to sell counterfeit merchandise, including clothing, shoes and jewelry. We also recently worked with the Federal Bureau of Investigation to disable the domain names of more than two dozen overseas websites that were selling counterfeit Tiffany & Co. jewelry. We are currently involved in an investigation by the Computer Crime Division of Scotland Yard to shut down websites that sell counterfeit tickets to sporting events. To date, we have successfully disabled access to approximately 60 such websites by redirecting their domain names. There are, of course, many more past and ongoing examples which would not be appropriate to disclose in this context.

We also continue to lead the charge to stop the proliferation of rogue online pharmacies and websites selling counterfeit medications. In 2010 alone we worked with the Federal Drug Administration and the U.S. Drug Enforcement Agency to investigate and take down over 36,000 such websites.

The Domain Name Registration Process

The domain name registration system is entirely automated. There is no human intervention into the process. Because many words have multiple meanings and combinations of words can be used for both legitimate and illegitimate purposes, no domain names are automatically prohibited from registration. As mentioned above, Go Daddy registers a domain name at a rate of more than one per second. This makes it virtually impossible for a human being to verify the legitimate use of every domain name

registration, particularly on an ongoing basis. To compensate for this, we have developed a notification system for reporting instances of all types of network abuse to our internal Abuse Department.

The Notification Process

With over 47 million domain names under management, most of our data come from third-party complaints or notices. The Go Daddy Abuse Department can receive information that ParaSites may be residing on our network in several ways: 1) direct complaint from a third-party via email; 2) direct complaint via telephone; 3) tip from Go Daddy employees who have either become aware of, or suspect the existence of, illegal content on a customer site; and, 4) notifications from CyberTipLine and other "watchdog" groups.

The Investigation Process

Once Go Daddy is made aware that a potential ParaSite is registered through one of our companies, we immediately investigate to determine whether there is in fact illegal content associated with the domain name, such as Scheduled drugs for sale without a prescription or child pornography (hereafter, "CP"), on the site. If so, we determine whether that customer has other domain names resolving to the ParaSite, and whether there are other ParaSites in the customer's account. In some cases, Internet users can only access ParaSites (such as sites containing CP) by supplying a paid-for membership user name and password. While we cannot investigate content that requires payment to access, we do investigate all web pages found to be freely accessible to Internet users without a user name and password for any site that we suspect is a ParaSite.

After we determine that there is content meeting the criteria for classification as a ParaSite, we archive a screenshot (in the case of a registered domain) and all or partial content (in the case of a hosted site) sufficient to demonstrate evidence of illegal activity for future use in law enforcement investigations.

The Suspension Process

After domain names, websites, and registrant information have been investigated and determined to be associated with illegal activity, we permanently suspend our services. It is important to note that domain names are not suspended prior to investigation, especially where domain names are not associated with an active website. It is very difficult for us to suspend a domain name before it is associated with an active website because many words have multiple uses. In addition, if there is no ParaSite associated with a particular domain name, there is no reason to suspend the domain name itself because there is nothing unlawful about a domain name, in and of itself.

Our Results

Go Daddy has documented proof that our efforts to preserve the safety and integrity of the Internet work. We investigate hundreds of thousands of domain names and websites each year for illegal activity. In 2010, we conducted approximately 672,000 investigations, involving approximately 40,000 unique customers.

The number of domain names and websites investigated each year is much higher than the number of unique customers investigated. This is because one unique customer may have many domain names. Many times, one customer will have literally hundreds of domain names in its account. In those cases, we suspend *all* the ParaSites associated with the customer's account, not just the ones about which we receive a complaint or notification. In 2010 alone, Go Daddy suspended approximately 150,000 websites found to be engaged in illegal or malicious activity.

Importantly, these numbers are skewed slightly lower because many times when Go Daddy is the registrar, but not the hosting provider, ParaSites have already been removed by the hosting provider by the time we conduct our investigation. This is a result of third-party complaints being sent to both the domain name registrar and the hosting provider at the same time, and illustrates the efficient results that can be obtained by providing concurrent notifications to all the Internet ecosystem players. We are, of course, very grateful when our fellow Internet companies take complaints of ParaSites as

seriously as we do and when they fully cooperate with us to terminate their services to ParaSites to help rid the Internet of illegal content.

Our Recommendations For Combating ParaSites

Go Daddy has a long history of supporting federal legislation directed toward combating illegal conduct on the Internet. For example, our company strongly supported the Ryan Haight Online Pharmacy Consumer Protection Act of 2008, which amended the Controlled Substances Act to significantly increase the criminal penalties associated with illegal online pharmacies. We also vigorously advocated for the passage of the Protect Our Children Act of 2008, which, among many other protections, prohibited the sending of live images of child abuse via the Internet, and authorized an additional \$320 million in funding for the fight against CP. Go Daddy always has and always will support both government and private industry efforts to identify and disable all types of ParaSites on the Internet. And, as set forth below, we have several specific recommendations that we believe will make the fight against illegal activity online more efficient and effective.

Direct Complaints Regarding Domain Names To Registrars Rather Than Registries

We believe that complaints against domain names should be directed to the appropriate domain name registrar, rather than to the registry. Because it is the registrar that typically has the most contact with the registrant of a domain name, registrars are very often involved in a variety of criminal investigations relating to websites associated with the domain name (for example, CP investigations involving registrants). The registry in many instances has no knowledge of these highly confidential and sensitive matters, and we have experienced several occasions in which the sudden disabling of a domain name by a registry disrupted weeks or months of work investigating serious criminal activity by the registrant. We would like to see future government and private industry efforts focused on naming the registrar as the primary contact for courts and law enforcement regarding all criminal and civil matters relating to domain names. We can then facilitate and coordinate concurrent actions by international, federal and local governments with respect to particular names.

Direct Complaints Regarding Illegal Content to All Relevant Members of The Internet Ecosystem

We further ask the Committee to consider establishing notice and takedown procedures, such as those provided for by the Digital Millennium Copyright Act (the “DMCA”), that could be applied to additional types of illegal content and to additional online service providers, including all members of the Internet ecosystem. While it is practically a mathematical certainty that the players and types of illegal content will change in the future, today the relevant members of the ecosystem would include registrars, hosting providers, payment processors, shippers, Internet service providers, search engines, and online advertising providers (hereinafter, the “Ecosystem Members”).

The DMCA provides a process for copyright owners to directly contact online service providers regarding websites that contain infringing material, and demand the removal of that content. The law establishes a safe harbor for providers that promptly remove the infringing material following notification, so long as the provider follows the processes outlined in the statute. Go Daddy has found the DMCA to be an extremely useful tool in combating online infringements and counterfeits, and has adhered to its provisions with much success. We have removed tens of thousands of websites that contain counterfeit or infringing material after receiving notification of the existence of the sites from third-parties pursuant to the DMCA. We anticipate that we would make even greater strides in this area if the DMCA were expanded (or new legislation were put into effect) to include notice and takedown provisions for illegal conduct other than copyright infringement – trademark infringement, for example, as well as spam, phishing, fraud, etc. The expanded legislation could and should apply to all of Ecosystem Members.

It is obviously critical that the Ecosystem Members all work together to combat ParaSites. To the extent that any Ecosystem Member receives notice that a member of its network is engaged in illegal conduct, that organization should be required (or, better yet, take it upon itself as the responsible thing to do) to disable access to the resources that are allowing the criminal to engage in the nefarious activity. With the help of clearly defined and widely disseminated notification and takedown procedures, the Ecosystem Members

should be able to cut off a large portion of the technical and financial resources that have, to date, allowed the proliferation of online bad actors. And, consistent with current law, future legislation should include an immunity provision for the “good actor” members of private industry that act in accordance with or exceed the law’s provisions.

Utilize DNS Blocking Instead of DNS Filtering To Combat ParaSites

Finally, Go Daddy has some concerns about recent proposals to impose domain name system (“DNS”) filtering as a means of combating ParaSites. We strongly prefer “DNS blocking” to “DNS filtering” as an effective strategy for disabling access to illegal and malicious content on the Internet.

The DNS is the standard technology for managing domain names on the Internet. DNS technology allows you to type a domain name into your web browser and locate the address, or URL, for that domain name. A “DNS server” is any computer registered to join the DNS. DNS servers run special-purpose networking software, feature a public IP address, and contain a database of network names and addresses for other Internet hosts. DNS servers communicate with each other using private network protocols.

All DNS servers are organized in a hierarchy. At the top level of the hierarchy, so-called “Root servers” store the complete database of Internet domain names and their corresponding IP addresses. The Internet currently employs 13 Root servers, located in various countries around the world. All other DNS servers are installed at lower levels in the hierarchy, and maintain only certain pieces of the overall database. Most non-Root DNS servers are owned by businesses or ISPs, such as Go Daddy and Google, and are maintained in various locations around the world.

The term “DNS filtering” describes a mechanism through which ISPs prevent outbound DNS inquiries regarding particular domain names from reaching the Root servers for those names. The net effect is to prevent the ISP’s customer base (i.e., only those customers that are using the ISP’s DNS servers) from being able to access the domain name or website in question. “Filtering,” rather than “blocking,” is the best name for this

mechanism, because the process does not and will not provide 100% protection. At best, it prevents a significant portion of a single ISP's customer base from being able to access a "DNS-filtered" ParaSite.

In our view, DNS filtering is an ineffective mechanism for fighting illegal activity online. The widespread implementation of DNS filtering would result in a large number of Internet users attempting to circumvent such filtering. While the easiest and most common way to do this is to use a proxy site, undoubtedly some users will change their primary DNS resolver to an overseas provider. If more users begin using DNS servers that are not secured, they will be in a position of exposed risk to DNS poisoning and similar security concerns. Ironically, this increases the likelihood of their exposure to ParaSites.

In addition, the imposition of DNS filters would diminish the ability of DNS providers in the United States to implement DNS security extensions, and of domestic ISPs and DNS providers to monitor DNS servers. Overseas DNS providers have not yet widely implemented DNSSEC authentication keys. Without such keys, providers have no way of verifying the validity of DNS record responses. As a result, if a significant portion of a provider's customer base uses other DNS servers as a rule, the provider will be unable to effectively protect those customers.

We believe that DNS blocking, as opposed to DNS filtering, is a much more effective vehicle for removing illegal content from the Internet. DNS blocking is different from DNS filtering in that DNS blocking is action taken at the "authoritative" or "response" level of the DNS cycle. As such, it needs to be done by the registrar (which provides the authoritative DNS response), or, in cases where the registrar is unable or unwilling to comply, by the registry (which provides the Root zone file records – the database -- for the entire TLD). Though a very similar technical process to DNS filtering, DNS blocking provides a much more thorough solution because it applies to all Internet users, regardless of which ISP they are a customer of or whether proxy services are used.

Where DNS blocking is imposed, Internet users will not be able to access a ParaSite by any common means.

Conclusion

Thank you again, Chairman Goodlatte, for the opportunity to testify on these important issues. Your commitment and the commitment of the Members of this Committee to bringing attention to the problem of ParaSites on the Internet is sincerely appreciated. Go Daddy is committed to working with you, with law enforcement, and with our fellow Internet Ecosystem Members to remove illegal content from the Internet.

I would be happy to answer any questions you may have.