Before the Congressional-Executive Commission on China

Hearing on "Google and Internet Control in China: A Nexus Between Human Rights and Trade?"

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

March 24, 2010

Introduction

Thank you, Chairman Dorgan, and members of the Commission, for the honor of testifying here today. We at Go Daddy applaud the actions of the Commission to support the continuing global exchange of information and trade on the Internet.

Background

The recent cyber attacks on Google and other U.S. companies are troubling, but they reflect a situation that The Go Daddy Group has been combating for many years. Go Daddy is an Arizona company which consists of eight ICANN-accredited registrars, including GoDaddy.com, Inc., the world's largest domain name registrar. This month, Go Daddy passed a major Internet milestone – we now have more than 40 million domain names under management, more than any other company in the history of the Internet. We are also the largest provider of shared website hosting. We have more than 7 million paying customers located all over the globe. So, if you are an active Internet user with a domain name or a website, the likelihood is that at some point you have utilized Go Daddy's services to engage on the Internet.

Go Daddy's customer base includes tens of thousands of Chinese nationals. We work with Chinese customers on a daily basis to help them to establish an identity on the Internet, and to ensure the secure and seamless operation of their hosted websites. We are also constantly in the process of repelling cyber attacks against the systems and infrastructure that secure our customers' websites and Internet activities. A large percentage of those attacks can be traced to China, as can other illegal activities that interfere with our customers' safe and productive use of the Internet. I am here today to share some of our experiences as they relate to China, specifically with respect to the following: increased monitoring and surveillance of .CN domain name registrations; increasing DDoS attacks originating in China; spam; payment fraud; and, what we would like to see the US Government do to help alleviate some of these issues.

Increased Monitoring And Surveillance of .CN Registrations

There appears to be a recent increase in China's surveillance and monitoring of the Internet activities of its citizens. As a domain name registrar, Go Daddy provides registration services for numerous top level domain names. Top level domains, or "TLDs," are the suffix that appears at the end of a domain name (for example, .COM, .NET, etc.). One of the TLDs we have historically offered is .CN, the Chinese country code top level domain (or "ccTLD"). Go Daddy is authorized by the China Internet Network Information Centre (known as the CNNIC), a quasi-governmental agency in China, to offer registration services for the .CN ccTLD. Go Daddy began to offer the .CN ccTLD in April of 2005 and, at this time we have approximately 27,000 .CN domain names under management. Registering a domain name with the .CN ccTLD is an important step for any individual or company wishing to establish an audience or business foothold in the Chinese market.

When Go Daddy started registering the .CN TLD in 2005, CNNIC required us to collect the contact information of the individual or company registering the domain name. The required contact information included first and last names of the registrant, his or her physical address, telephone number and email address. The extent of the personal information collected was typical of what is normally required by .ccTLD registries.

A little over four months ago, on December 12, 2009, CNNIC announced that it was implementing a new policy relating to the registration of .CN domain names, and that it would begin to enforce the new policy effective December 14, 2009. The policy required that any registrants of new .CN domain names provide color headshot photo identification, business identification (including a Chinese business registration number), and physical signed registration forms. This information was to be collected by the registrar, and then forwarded to CNNIC for its review prior to the activation of the registration.

Less than a month later, on January 5, 2010, CNNIC announced that Chinese nationals were no longer permitted to register domain names through non-Chinese registrars. In accordance with the new policy, Go Daddy halted all new .CN registrations.

On February 3, 2010, CNNIC announced that it would reopen .CN domain name registrations to overseas registrars. However, the stringent new identification and documentation procedures would remain in effect. CNNIC also announced an audit of all .CN domain name registrations *currently* held by Chinese nationals. Domain name registrars, including Go Daddy, were then instructed to obtain photo identification, business identification, and physical signed registration forms from all *existing* .CN domain name registrants who are Chinese nationals, and to provide copies of those documents to CNNIC. We were advised that domain names of registrants who did not register as required would no longer resolve. In other words, their domain names would no longer work.

We were immediately concerned about the motives behind the increased level of registrant verification being required by CNNIC. It did not make sense to us that the identification procedures that had been in place since 2005 were apparently no longer sufficient from China's standpoint, and no convincing rationale for the increase in documentation was offered. We were also concerned by the *ex post facto* nature of the new requirement – in other words, at the time the affected Chinese nationals registered their domain names, they were not required to provide photo identification and the other documentation now being required by the CNNIC. The new documentation requirement was to be retroactively applied to registrants who had previously registered their websites, in some cases years before. The intent of the new procedures appeared, to us, to be based on a desire by the Chinese authorities to exercise increased control over the subject matter of domain name registrations by Chinese nationals.

Approximately 1,200 unique Go Daddy customers were affected by CNNIC's *ex post facto* application of the requirement for additional identification documentation. This represented a much larger number of domain names, of course, because many registrants

have multiple domain names under their control. We contacted our affected customers advising of this new requirement, and advised them that, if they wished to provide us with the required documentation, we would provide it to CNNIC in accordance with CNNIC's directive. Ultimately, only about 20% of the affected customers submitted the required documentation and agreed to allow us to submit it to the CNNIC. The domain names of the remaining 900 or so customers remain at risk of cancellation. That means thousands of websites the Chinese authorities may successfully disable because of retroactive application of this new set of rules.

Go Daddy has been registering domain names since 2000. We currently serve as an authorized registrar for dozens of domain name extensions. This is the first time a registry has asked us to retroactively obtain additional verification and documentation of individuals who have registered a domain name through our company. We are concerned for the security of the individuals affected by CNNIC's new requirements, as well as for the chilling effect we believe the requirements will have on new .CN domain name registrations. For these reasons, we have decided to discontinue offering new .CN domain names at this time. We continue to manage the .CN domain names of our existing customers.

Increasing DDoS Attacks Originating in China

Another China-related issue we have seen recently is an increase in the number of distributed denial of service (also known as "DDoS") attacks on the systems that host our customer websites. In Go Daddy's case, a DDoS attack is typically an attempt to make websites that we host unavailable to their intended users for some period of time. We also combat many attacks that are more systematic, such as hackers attempting to insert malicious code into the pages of our customers' hosted websites. An example of this type of attack would be the installation of spyware on the computers of all visitors to a website we host. The spyware then logs keystrokes to harvest passwords to email accounts, which can then be infiltrated and monitored without the knowledge of the account owner.

Go Daddy operates data centers, and has invested hundreds of millions of dollars in those centers, including building and operating state-of-the-art security measures that monitor and fight external attacks on our systems 24 hours a day, 365 days a year. In the first three months of this year, we have repelled dozens of extremely serious DDoS attacks that appear to have originated in China, based on the IP addresses from which the attacks derived. Had our security systems not countered these attacks, the result would have been a widespread take-down of our customers' hosted websites.

Spam

Unlike many other Internet companies of our size, Go Daddy operates a large 24/7 Abuse Department whose mission it is to identify and help stop illegal and malicious activity on the Internet. We work very closely with local, federal and international law enforcement agencies to stop all types of Internet abuse, including child pornographers, unauthorized online pharmacies, spammers, phishers, and sellers of counterfeit merchandise.

In monitoring spam activities, we have found that an overwhelming majority of websites promoted through spam are hosted in China, often at service providers that choose to ignore complaints of spam and other types of illegal activity. When Go Daddy and other legitimate hosting companies receive complaints that spam is being sent from websites hosted by their company, the sites are typically taken offline. However, many companies in China offer so-called bulletproof hosting, where websites are allowed to stay online and spam operations can continue unabated, even after receipt of a complaint.

China is also the location of choice for buying and selling lists of spam "zombies" - personal computers deliberately infected with spam-enabling viruses and operated by ordinary, usually oblivious, computer users around the world. Our research indicates that China dominates the market for buying and selling lists of zombie PCs, which are peddled by virus writers on Internet forums found on Chinese servers. Lists can currently be had for about $2,000-$3,000 per 20,000 compromised computers.

Another reason so much spam appears to originate in China is the spam industry's growing sophistication. The modern spam industry is populated by technically advanced programmers and organized crime rings. Spammers create complex phishing scams to lure individuals to fake websites where they are conned into divulging bank account, social security and credit card details. Organized spam groups tend to avoid operating in jurisdictions where authorities are hostile and penalties potentially severe. To date, China has not enforced significant penalties against spammers and others who utilize the Internet to engage in criminal activities; thus, it has become a sort of safe harbor for such criminals.

China is also an attractive locale from which spammers operate because of its low costs. A domain name can be bought for as little as $0.15 in China, which allows scammers to acquire lots of domain names inexpensively. Domain names cost much more in the United States, where some of the money goes to fighting abuse and spam. But the low revenue stream in China is likely hampering the creation of programs to stop abuse.

China today is basically the only major market where spammers can do just about anything they want. Go Daddy's efforts to persuade authorities there to investigate or prosecute spammers have been ineffective, as have our efforts to work with Chinese-based hosting companies to shut down compromised websites. Official pronouncements by the Chinese government usually appear to be aimed at getting Chinese spam servers removed from foreign blacklists rather than actually preventing spam.

Payment Fraud

In addition to our Abuse department, Go Daddy also has a full time Fraud department that is continually monitoring and guarding against payment fraud issues affecting our customers. The payment fraud trends associated with China-based users include the widespread use of compromised U.S. or UK credit cards to purchase items. In one particularly egregious case, an individual or group operating from China is utilizing compromised credit cards from a wide variety of banks to purchase one year domain name registrations. The registrant then attempts to use the domain names to perform a

variety of illegal activities. Since January, our Fraud team has managed to close 134 new shopper accounts associated with this repeat Chinese fraudster.

Go Daddy has also been successful in combating Chinese spammers by closing customer accounts through our payment fraud process. Most recently, our Abuse department identified a Chinese-based spammer with 175 separate shopper accounts with Go Daddy. Although each of the accounts was opened using a valid PayPal account, we were able to halt the spammer's activities by placing a payment fraud lock on the accounts.

In addition to the challenges presented by China-based criminals, societal and cultural norms in China can make it difficult to identify and resolve payment fraud issues affecting legitimate Chinese customers. For instance, a problem we frequently encounter is the provision of invalid shopper/billing information by Chinese shoppers. Where invalid information is provided, contacting the customer to verify order activity is usually impossible.

Credit card use is not prevalent in China, and most Chinese shoppers do not possess their own credit card. When credit cards are issued, they are often shared by numerous individuals. It is therefore very common for accounts owned by Chinese shoppers to have multiple unrelated names and addresses on file. This too makes identifying payment fraud more difficult.

Despite these payment fraud challenges, Go Daddy is focused on continuing to serve and expand upon its Chinese customer base. In furtherance of this goal, in December 2009, we began to offer the Alipay payment processing system to our customers. Alipay is China's leading independent third-party online payment platform, with more than 270 million registered users. What sets Alipay apart from other online payment platforms is that it holds funds in escrow until the product is received. Chinese customers can fund their Alipay accounts using direct bank payments or debit cards, both of which are more common forms of payment in China than credit cards. Alipay is a popular and trusted option for Chinese consumers, and we have experienced a large increase in our volume of

sales to Chinese customers since we implemented it as a payment option. We have also found use of the Alipay system to be very helpful in combating China-related payment fraud. In fact, our new shopper payment fraud rates associated with Chinese accounts has been reduced by approximately 50% since we introduced Alipay in December of 2009.

What the U.S. Government Can Do To Help

Go Daddy's primary mission is to promote secure, easy, equal access to the Internet to people around the world. We are also committed to ending illegal or nefarious uses of the Internet, including for the invasion of personal privacy or to limit freedom of expression. We believe that many of the current abuses of the Internet originating in China are due to a lack of enforcement against criminal activities by the Chinese government. Our experience has been that China is focused on using the Internet to monitor and control the legitimate activities of its citizens, rather than penalizing those who commit Internet-related crimes.

We believe that countries or individuals that engage in cyber attacks or other types of Internet crimes should face serious consequences and international condemnation. We hope that the U.S. government can use its influence with authorities in China to increase Chinese enforcement activities relating to Internet abuse, while encouraging the free exchange of ideas, information, and trade. This would include the retraction of China's recent policies relating to the registration of .CN domain names, which will act as a barrier to Internet access by Chinese nationals.