Remarks by Director John Morton
U.S. Immigration and Customs Enforcement
Department of Homeland Security
State of the Net Conference
Washington, D.C.
January 18, 2011

Good morning, I am indeed John Morton, Director of Immigration and Customs Enforcement, or ICE. A quick primer on ICE. ICE was created in the aftermath of 9/11 by merging the investigative arms of the United States Customs Service and Immigration and Naturalization Service. We are a large agency with 20,000 employees, a budget of about 5.8 billion dollars, and offices in all 50 states and 46 countries overseas. Our enforcement jurisdiction is quite broad and covers everything from drug, firearms, and smuggling, to money laundering and child exportation.

So why is the head of a federal agency with jurisdiction over customs, immigration, and border crimes appearing at a

conference titled "State of the Net." What does ICE have to do with the internet?

I am here because my business—investigating crime—has brought me to the net. Crimes that in the past occurred almost exclusively on the street or through the mails—counterfeiting, child pornography, copyright infringement—now take place in cyber space. I am here because the internet has changed ICE's world as well as yours.

I am not here because I believe the internet is a bad thing. It's not. It's one of the great advances of our time and will shape our lives and those of our children without any doubt. I am here to emphasize that good law enforcement now requires investigation on and through the web. It's enforcement that protects the internet from crime and exploitation; it's enforcement that should receive strong public support.

Let's take child pornography, for example. In the old days, child pornography typically involved the sharing of illicit photographs or movies by mail. Today, almost all of this illicit activity has moved to the internet. Instead of working mail rooms and shipping centers, we know work websites, chat rooms, and on-line networks.

Sadly, there is no shortage of work. ICE, working with the Justice Department, charges about 1,000 child exploitation cases a year—the vast majority child pornography cases involving the internet. In a subset of cases, active physical abuse is present: videos of child abuse, attempts to lure children into having sex, web pages promoting child sex tourism overseas.

In the fraud realm, ICE, and other federal law enforcement agencies, pursue individuals who defraud credit cards companies by establishing accounts with stolen

identities, some gained through "phishing" scams. Goods are illegally bought from legitimate internet sites with fraudulent credit cards in the U.S. to be shipped to foreign fencing operations, leaving the individual whose identity has been stolen, the credit card company and the internet merchant as domestic victims.

And as all well know, intellectual property theft has migrated to the internet as well. Whether it is online sites that offer fake luxury goods for sale or pirated movies, music and software, there is a virtual flea market that has become a seamy side of the internet.

This side has unfortunately grown as access and bandwith have increased. The *2010 Cisco Visual Networking Index* that reports download speeds of DVD quality movies have been reduced from taking three days 10 years ago to

around two hours last year. MP3 audio download time has been reduced from three minutes to about five seconds. The same report forecasts that global IP traffic will quadruple by 2014.

Increases in speed and access to the Internet, while valuable for global communication and commerce, also provides criminal opportunity for those poised to take advantage of it, and presents a real risk to America's film, television, and music industries. Because of their digital capability, their products are extremely susceptible to Internet theft, and will continue to be so as bandwidth increases. As a result, our IP investigations are increasingly directed toward Web-based criminals.

Let me discuss briefly the most recent enforcement action undertaken specifically to address intellectual property theft online. Through Operation In Our Sites, and the word

"sites" is spelled s-i-t-e-s as a purposeful play on words, federal magistrate judges issued criminal seizure warrants for the domain names of websites that illegally offered copyrighted or trademarked goods without authority of the rights holder. ICE investigated the websites and in all cases obtained counterfeit trademarked goods or pirated copyrighted material. The evidence collected during the investigation was presented to attorneys with the Department of Justice, who worked with the ICE agents to determine whether to obtain seizure orders for each site.

Among the determinations for the ICE agents and the prosecutors were whether the domain names are of course registered here in the United States, which as many of you know all DOT NETS (.nets) and DOT COMS (.coms) are, even if the website is operated overseas. The court orders were served by ICE agents on the domestic domain name registries and the domain names were seized and the sites

redirected to a contract server. The contract server links the domain name to a new site that includes only a seizure notice advising anyone who sees it that a federal court order has been issued for the domain name.

As with any other court order, the owner of that domain name may challenge the seizure warrant through petition to the U.S. District Court in which it was issued. A hearing would then be held at which the site owner would appear and have counsel present, if they so desired. The government would have the burden of proof and present our evidence so that the court could determine the validity of the affidavit that had initially supported the seizure.

During the first phase of In Our Sites last June, ICE and the U.S. Attorney for the Southern District of New York obtained seizure warrants for domain names of eight websites offering pirated films and TV programs. These sites allowed

visitors to stream or illegally download current, highly popular television shows and movies. The sites we targeted offered more than 200 movies – often within days of theatrical release – and more than 300 television programs. Of great interest, and frankly unanticipated, was the collateral impact of this enforcement action.

According to industry analysis, 81 other sites that had been offering pirated material voluntarily shut themselves down. In my many years in law enforcement, I have not seen that type of deterrence. Indeed, we were advised that seizing these domain names would be the proverbial "Whack a Mole" game with new ones popping up faster than we could obtain court orders. That did not occur and while two of the original domain names seized did reemerge in another form, the vast majority did not and two months ago, we seized one of the two that had been resurrected and was offering pirated movies again. It has not reemerged since.

Our seizure banners, now in place of the illegal material, have received over 25 million "hits." In some cases receiving more visitors than the sites were when they were offering content and counterfeit goods illegally.

Operation In Our Sites will continue periodically through the year as the rights holders of trademarks and copyrights refer offending websites to ICE and the Department of Justice. Importantly, in the last round of Operation In Our Sites, the private sector referred over 130 websites for action, but ICE agents through their investigation, narrowed this list considerably and court orders were executed against 82 sites. So while industry can refer, law enforcement and the federal court system have the responsibility to determine which are engaged in illegal conduct.

Why will we continue with these operations? Why do we, as a law enforcement agency care? Why is the Department of Homeland Security engaged in this type of enforcement activity? These are questions that have been asked. Let me try in the brief amount of time I have to offer some insight.

The vast majority of commerce on the internet is legitimate—real goods, real vendors, albeit in the virtual world. But there are those fake goods, fake vendors, and individuals not only do not contribute to legitimate commerce on the internet, but rather take away from the image of the internet as a safe and convenient place to shop. They chill the sense of freedom that someone might have shopping from their home for a reliable and legitimate product.

Remember counterfeiters and copyright infringers are not good corporate citizens. They are not invested in

American economic growth, innovation, or brilliance. They don't pay healthcare, taxes, or pensions. They don't invest in the next movie, the next revolutionary drug, the next technological advance. No, they wait for others and profit, criminally, without doing any of the work, any of the thinking.

Our intellectual property enforcement on the internet has been alternately praised by victim rights holders, criticized by some, and watched with curiosity by many. We respect the debate and will withstand the criticism. Importantly, people should understand three things: First, ICE is not the police of the internet. Second, we are not interested in limiting speech or due process. Third, we will follow criminal activity wherever it occurs, including the internet. In short, we are going to stay at it. I am unapologetic on that last point, just as we are when a crime occurs at our physical border, in your

home, or at the proverbial corner of Fourth and Main. Crime is crime.

So with that, thank you for your time today. I have another appointment this morning and need to depart in a few minutes, but I'd be happy to take a question or two before I have to go.