TESTIMONY OF

Special Agent Flint Waters
Lead Agent for the Wyoming Internet Crimes Against Children Task Force

WYOMING DIVISION OF CRIMINAL INVESTIGATION
OFFICE OF THE ATTORNEY GENERAL

for the

UNITED STATES SENATE
COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON CRIME AND DRUGS

"Challenges and Solutions for Protecting our Children from Violence and Exploitation in the 21st Century"

April 16, 2008

Chairman Biden, Ranking Member Sessions, distinguished Senators, thank you for the opportunity to testify before you today on the subject of violence and exploitation against children. I am Flint Waters, Special Agent with the Wyoming State Division of Criminal Investigation. We are home to the Wyoming Internet Crimes Against Children (or "ICAC") task force. We also developed child exploitation investigation software and host the undercover infrastructure that is used by law enforcement agencies throughout the United States and the world.

I am here today first as a front-line investigator—as an officer who is on the ground, pursuing these cases, serving the warrants, arresting the offenders and rescuing the children. I see the challenges first hand.

I am also here today to offer my insight from a broader perspective. Because of Wyoming's role in research, development and deployment of anti-child exploitation programs and systems, we see a "big picture" that was not visible just three years ago.

Our system, known as "Operation Fairplay," is housed by the State of Wyoming and used throughout the world. It is a comprehensive computer infrastructure that gives law enforcement the tools they need to leverage the latest technologies to identify and track those who prey on children, just as the offenders use technology to identify and track the children that would be their prey.

The Wyoming system has enabled law enforcement to begin to bring into focus a picture of the staggering magnitude of child pornography trafficking today. Along the way, we have learned a great deal about how law enforcement can effectively fight back, interdicting hundreds of thousands of criminals and rescuing countless children. When I

am not working these cases, I am training investigators from around the world to do what we do.

Through this system we are able to deliver solutions that help investigators working peer-to-peer, chat room, online gaming and mobile phone undercover operations.

With the rise of the Internet, child pornography trafficking has exploded, both commercially and non-commercially. I want to emphasize at the start the importance of responding to this problem with a multi-pronged attack. The National Center for Missing and Exploited Children, through its CyberTip hotline, is serving the critical task of receiving the 911 calls for help from citizens and Internet service providers (ISPs). As you know, having someone there to respond to these reports of suspected criminal activity is essential if we hope to make use of this valuable resource.

Of course, it is also essential that law enforcement—to include state and local law enforcement agencies, the Internet Crimes Against Children Tasks Forces, the FBI Innocent Images Initiative, the Department of Homeland Security and the US Postal Inspection Service—be ready not only to respond to these public reports, but to aggressively mount a proactive attack as well. We can not carry this fight without both a defense and an offense.

Let me share with you some of the material we see every day:

One of the most frequently seen movies being distributed now is of a toddler on a changing table. The video zooms in as the child's diaper is removed and an unknown male penetrates her. We are seeing the rape of more and more extremely young children like this. Criminals are even using live web casts, where online participants direct what is done to the child. We trace this activity into our own states and rescue children in our own communities.

We are also seeing modifications of these movies and images. Offenders are compiling the material in online instruction manuals, training each other how to rape children in ways that make it more difficult to detect, in ways that are harder to prove during medical examinations.

If you want to see how these methods work, consider some of the children we have already rescued and those where we were too late. In San Diego our system resulted in the arrest of a respiratory therapist at a children's hospital. This offender was molesting children that were in his care, often hospice care. The victims he targeted were often non-verbal, representing the most defenseless, the most helpless children he could find. This isn't the type of person that is going to show up to meet Dateline. This is a person that already has access to children. He goes online and trades these horrific movies to normalize his decision to victimize one child after another. Shortly after his arrest two of the children he had been victimizing died.

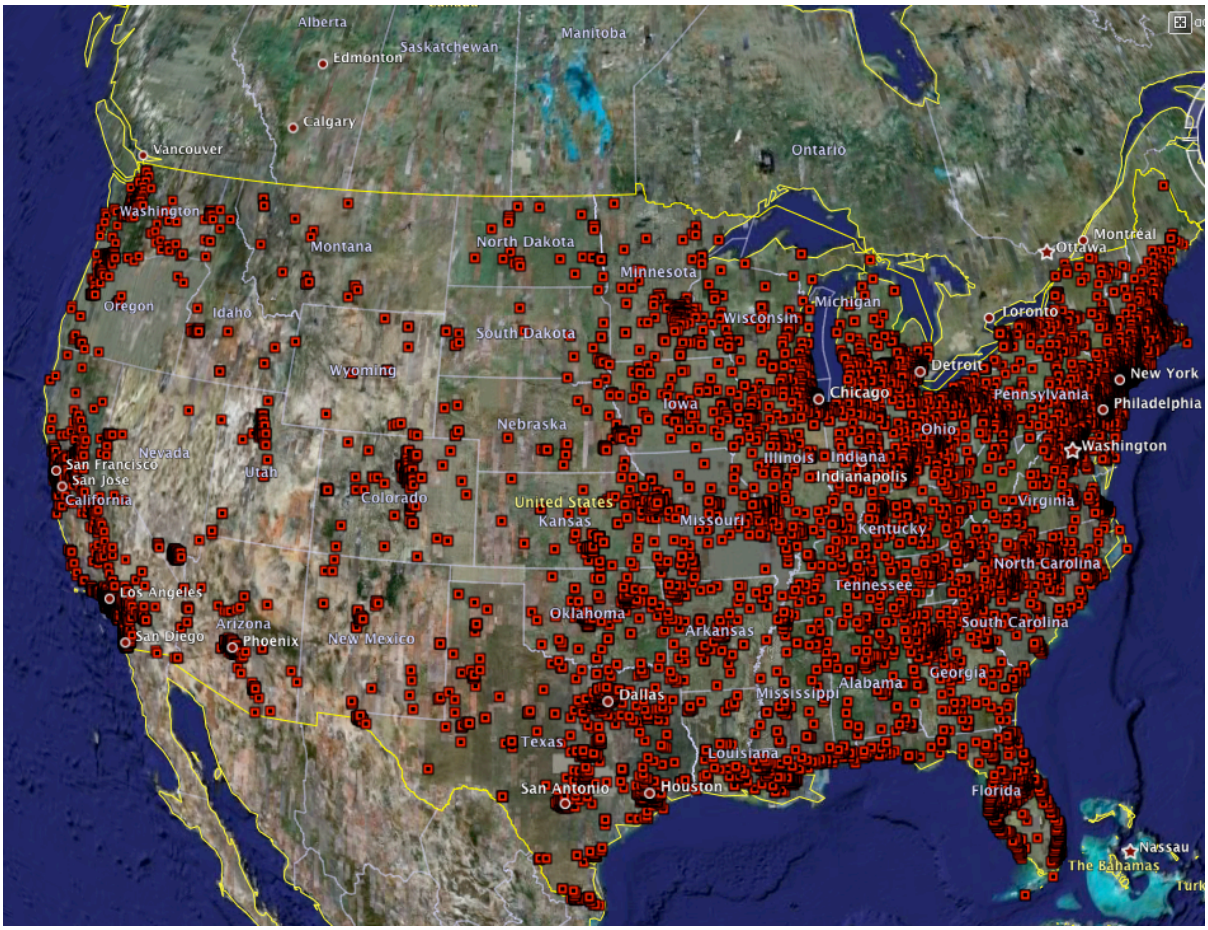
Using data modeling features in Fairplay we were able to find an offender in Ohio who had been seen over 800 times. This monster would film himself drugging the juice boxes of neighborhood children. He would film himself tricking them into drinking the juice. Next he would film himself as he raped the children. Numerous children were rescued because this predator traded child pornography on the Internet. Intervening on behalf of these children is more than working in chat rooms, or web sites, or peer-to-peer. It is about placing law enforcement in every possible forum where the offenders are leveraging technology to isolate and victimize children.

We can't blame the peer-to-peer systems. We can't blame chat rooms or social networking sites. We are a society of technological advance. Sadly, some leverage those advances to hurt children. Blaming this problem on peer-to-peer innovation is like blaming the Interstate highway system when someone uses it to transport drugs.

What we have to do is scale our law enforcement, prosecutorial and judicial resources to ensure we, as a society, are prepared to respond to the challenges that come from innovation, that we are prepared to rescue children when the map to their abuse is sitting right in front of us.

We need to insure that the national computer forensic capacity can recover and present the evidence of these crimes. Not just the FBI regional computer forensic labs but also partner solutions like the National Computer Forensic Institute in Alabama.

In the twenty-four hours preceding the submission of this testimony we found individuals trading this material all over the United States.



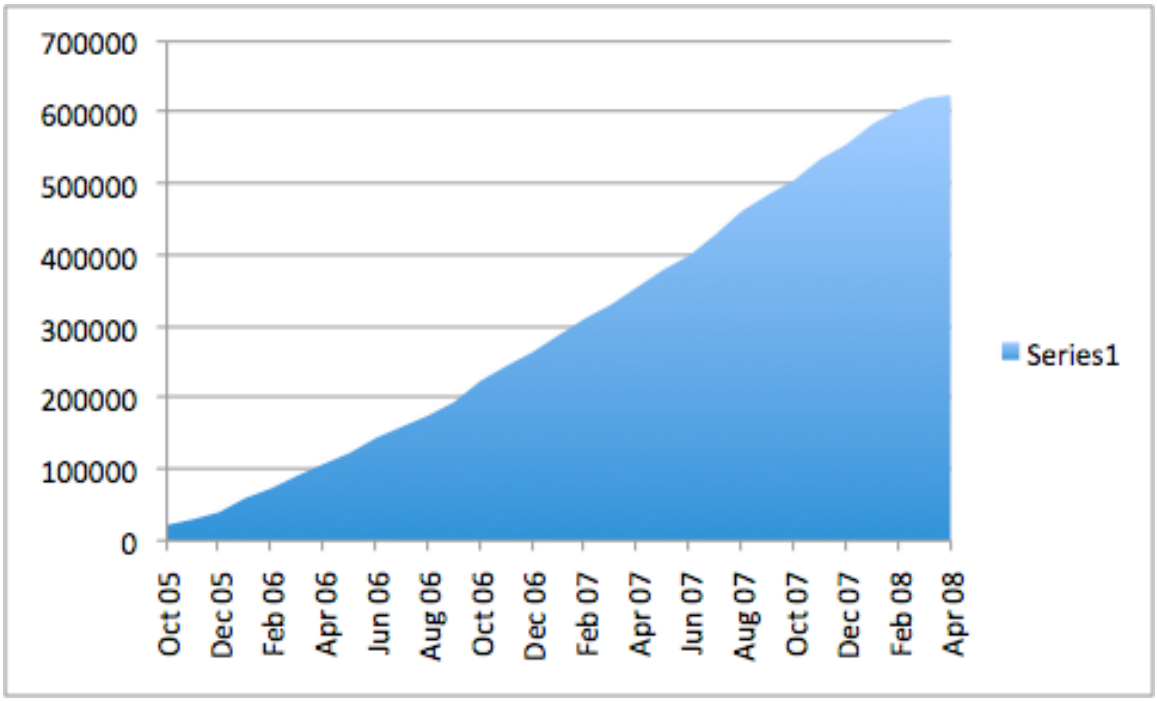
To better understand how many offenders we could investigate if we had the resources please consider these details:

In 2008 alone we have seen over 1,400 IP addresses that have been found by law enforcement 100 or more times. Imagine how many offenders have exchanged files with these top traders. The number next to the state only identifies how many times law enforcement saw the computer, not the offenders trying to trade child pornography.

2792	US,PA	759	US,FL	597	US,OH
1182	US,NJ	754	US,WA	590	US,NY
1076	US,MS	749	US,NC	557	US,VA
1049	US,TN	707	US,IL	556	US,IN
892	US,TX	703	US,AL	554	US,TX
889	US,MN	691	US,VA	551	US,NY
881	US,AZ	642	US,NH	551	US,CT
862	US,IN	631	US,LA	544	US,FL
841	US,NH	629	US,GA	536	US,PA
828	US,WA	629	US,CA	531	US,CA

824	US,MD	611	US,KY	529	US,NY
794	US,KY	607	US,MI	516	US,NY
772	US,VA	601	US,MN	516	US,MI
768	US,AZ	601	US,NY	509	US,TN

The identification of unique serial numbers that can be traced to the United States is still on the rise. Currently we only capture the serial number in about half of our undercover communications. We have exceeded 624,000 unique serial numbers that we can trace to the United States. We have 650,000 additional serial numbers that we cannot trace nationally because of the type of IP address they use. Typically over 40% of all leads trace to the United States. While we can speculate that another 260,000 unique computers are within the U.S. we are unable to be certain so we do not include them in this calculation.



Series one represents the progressive increase of unique serial numbers seen since we started widespread capturing of these details in Oct, 2005.

As you have seen the new technologies we have developed give us the unprecedented ability to locate and stop hundreds of thousands of suspects, before another child is targeted. Unfortunately, facing the scope of this problem can prove daunting.

I would like to be clear, I am NOT saying law enforcement isn't doing enough with what they have. I am saying they could do so much more if they only had the resources.

Senators, I would ask you to picture the pile of work you have to leave waiting at the end of your day. While you want to make more progress at some point you have to go home,

as it is there isn't enough time for home and family. Now imagine that in your inbox are hundreds of leads. And as you leave the office to go home, you know you are walking away from dozens of children who are waiting to be rescued. Each of those children must wonder if anyone cares.

Imagine if a serial rapist was on the loose in the U.S. attacking innocent citizens and then uploading videos of those rapes onto the Internet. That's exactly what we see flooding the Internet now. But the sexual assault victims are children. Many are infants and toddlers. Some cry and scream for help. Others have stopped crying.

Please forgive the offensive nature of what I am speaking about here today. I describe these despicable crimes to you because I hope that you never have to see them. I want you to truly understand the crimes being perpetrated on American children because I know that you have some of the greatest power to intervene.

Thank you for your time and attention on this matter.