Moderator: John T. Picarelli, Social Science Analyst, International Center, Office of the Director, National Institute of Justice, U.S. Department of Justice, Washington, D.C.

Panelists:

- Catherine J. Cummings, Executive Director, Financial Coalition Against Child Pornography, International Center for Missing and Exploited Children, Alexandria, Va.
- Bjørn-Erik Ludvigsen, Police Superintendent, National Criminal Investigation Service, Oslo, Norway
- Per-Ake Wecksell, Detective Inspector, Swedish National Criminal Police, Stockholm, Sweden

John T. Picarelli, National Institute of Justice, U.S.

John T. Picarelli: ... interest of trying to keep us on time, I'm going to get started in the hopes that well have a few late stragglers, but that's OK.

[Inaudible]

Picarelli: Excuse me?

[Inaudible]

Picarelli: You want me to speak like this? OK.

[Laughter.]

Audience Member 1: Just speak up.

Picarelli: Hi everybody.

[Laughter.]

Picarelli: I'm John Picarelli. I'm with the National Institute of Justice and its International Center. And its my privilege to welcome you to this panel today on the International Trends in Fighting Child Pornographym, as one of my colleagues has corrected me.

This panel came about mainly because of the mission of the International Center. The mission of the International Center at NIJ is two-fold. One, of course, is to focus on international criminal issues, and I can think of no other issue that is more international and more internationally challenging than child exploitation. And the other is to act as a bridge between the United States and foreign countries in the importation and exportation of both ideas and technologies. And what we have here today are three panelists that represent that ideal that both through their concepts and through the use of technology are building international coalitions in order to fight child exploitation online.

And so today what you will hear is the truest form of what we call ideas across borders. The idea that borders may act as an inhibitor at times but we need to transcend those borders in order to deal with many different forms of crime. So today well have three speakers. The first is Catherine Cummings. She's the executive director of the Financial Coalition Against Child Pornography at the International Center for Missing and Exploited Children, which is closely associated with the National Center for Missing and Exploited Children, right here in Alexandria, Va.

Then, after Ms. Cummings speaks, well have Bjrn-Erik Ludvigsen, who is a police superintendent with the National Criminal Investigative Service in Norway, but also serves as one of the coordinators for what is known as CIRCAMP, the COSPOL International --Internet-Related Child Abusive Material Project. COSPOL is another acronym that's basically an effort through the European Chiefs of Police Task Force in order to focus on criminal issues that transcend national borders in Europe. So this is one of these thematic networks, and Bjrn-Erik will go into more detail on how that works.

And then following Bjrn-Erik, well hear from Per-Ake Wecksell, who is a detective inspector with the Swedish National Criminal Police in Stockholm. Per-Ake is in a position — a more interesting position in that he's working with both. He is the primary liaison for the CIRCAMP effort in Sweden, but because of the Financial Coalitions work within Sweden, he has had contacts with them as well. So hell focus most of his remarks on CIRCAMP, but you may hear him mention how the Financial Coalition operates in Sweden.

So each will have 20 minutes to speak. Afterwards we should have about 20 to 30 minutes for question and answer, so I hope you'll have plenty of good questions to throw at them. So without further ado, Ms. Cummings ...

Catherine J. Cummings, Executive Director, Financial Coalition Against Child Pornography, International Center for Missing and Exploited Children, Alexandria, Va.

Catherine J. Cummings: Good afternoon everyone. I appreciate the introduction from John, and I appreciate the opportunity to speak with you this afternoon about a very critical problem that many groups are fighting globally. The group that I will describe to you is the Financial Coalition Against Child Pornography. It started in 2006, largely as a U.S. initiative, although we do have a good number of global companies involved. Were very active now and expanding the network and the concept to other parts of the globe. And its very nice to see my colleague from Sweden, Per-Ake, because we've seen each other at a couple of meetings in Stockholm, which is a very nice city, by the way.

So what Id like to do is just tell you quickly about the sponsoring organizations for the coalition, and then a little bit about the problem were trying to solve, and then Ill tell you about the coalition.

As John mentioned, the National Center for Missing & Exploited Children is based just down the highway in Alexandria. I would assume that some of you in the room are familiar with this organization, since we work very closely with the Department of Justice and the Department of

Homeland Security to provide services for families and law enforcement in the United States. The National Center is celebrating its 25th anniversary this year and plays a role, or originally was started to play a role to link law enforcement across the country so that everyone could do a more effective job of helping to find children who had been abducted and gone missing.

The group has expanded its mandate, and in addition to supporting law enforcement and missing children, we also focus on child sexual exploitation issues. In 1998, the United States Congress asked the National Center to set up a hotline, or a 911 for the Internet, which we call the CyberTipline. The CyberTipline receives reports from the general public and Internet service providers when they find suspicious sites or other elements that have to do with child exploitation on the Internet.

The sister agency is the International Centre for Missing & Exploited Children, also based in Alexandria. We work to combat child abduction and child sexual exploitation globally. Some of the ways we do that is by providing training and assistance to law enforcement, legal professionals, governments, and NGO's around the world, as well as advocating for changes in laws, and treaties, and systems to help protect children worldwide.

A quick side note, particularly since so many people at this conference have a background and an interest in research. The International Centre compiled a study and released it, initially in 2006, and it actually has been updated five times. You can find it on the Web site: www.icmec.org. This is a study of child pornography laws around the world in 187 Interpol member countries, and what we found is more than half have no laws at all that speak to child pornography specifically. So part of our work is to try to build a global landscape that is more consistent and more effective when it comes to fighting child pornography.

A little bit about the problem. The Financial Coalition Against Child Pornography is focused on commercial child pornography. There is a very robust trade of these images and videos between the offenders or the fans of this stuff where no money changes hands. Its peer-to-peer trading and things like that. What we focus on is the commercial — a lot of times its organized crime that collects these images and sells them, or collects these videos and sells them for subscription prices, and people buy monthly or yearly subscriptions to these Web sites.

It is a global problem. It has been fueled by electronic payment tools like credit cards, debit cards, PayPal, Western Union, as well as newer currencies that are popping up. When we talk to people about this problem — I doubt this is true with this group, but other groups will say to me, Well, isn't this really adult entertainment or adult pornography where women might be dressed up to look like teenagers or underage girls? And that is not the case. Tragically, there is a study recently done that the National Center was affiliated with, that looked at the images held by the people arrested. And 83 percent of those arrested were holding images of children 6 to 12 years old; 39 percent had images of children 3 to 5 years old; and 19 percent had images of infants and toddlers under the age of 3 being raped and sexually abused. And probably the individuals who are on the front lines fighting this will tell you that those trends are getting worse and not better.

Why is this a business? Why do we put together a coalition of Internet and financial companies that has anything to do with child pornography? If you can step away from the emotion of the

problem and look at it from an economic standpoint, children around the world are plentiful and easily accessible, unfortunately. Child pornography is easy and inexpensive to produce because of technology today. There is a very significant consumer market for this in the United States and outside of the United States. It is enormously profitable, and there's virtually no risk, although I can tell you point number five, we are changing that through the very concerted efforts of law enforcement around the world, as well as help from private industry, which is where we come in.

These are some of the solutions to fight the problem. And I'm going to talk to you about the last bullet. The Financial Coalition Against Child Pornography has one goal, which is to disrupt the economics of this business. Law enforcement, arrest, prosecution is always the first priority in anything we do, but this is a civil initiative. So it was formed on the premise that we cannot arrest and prosecute our way out of this problem. So in 2006, Senator Richard Shelby of Alabama, who at the time was the head of the Senate Banking Committee, convened a meeting of some of the credit card and financial companies and said, If we were buying and selling heroin and cocaine over the Internet and people were using their credit cards, we would do something about it, and this is far worse.

So, I am happy to report that the companies have stepped up to the challenge. This is a list of our current members, and it might be hard to read so Ill read off some of the names for you: the American Express Company, Banco Bradesco of Brazil, Capital One, Citigroup, Deutsche Bank Americas, Discover, Google, HSBC North America, JPMorgan Chase, MasterCard, Microsoft, PayPal, Visa, Wells Fargo, Western Union, and Yahoo!. Importantly you'll see its a collection of Internet companies and financial companies because together we all do a much better job of fighting this problem. Each of the companies on the list does whatever they can to fight the problem but we have learned that we can really make much more progress if we share information and help one another.

In 2006, the first priority was to develop a process for undercover credit card transactions in collaboration with law enforcement. A little bit of background. If a company like Visa or MasterCard or one of the banks suspects fraudulent transactions on their system, the security and risk people at those companies will do an undercover transaction themselves to follow the flow of funds and find the bad players who are in the payment stream. In the United States the mere attempt to purchase child pornography is a crime. So if you're working for MasterCard's security department, you cant do an undercover test transaction or you're going to have the FBI knocking on your door saying, You have an employee who is trying to access child pornography.

So because of the relationships that the National Center for Missing & Exploited Children had and has with law enforcement, we were able to recruit Immigration, Customs and Enforcement, FBI and some other law enforcement agencies to help us out with undercover transactions. Then we built out that tip line that I mentioned to you, to accommodate information from the financial companies. Something that I want you to keep in mind is that all of the sharing of the data is well within privacy and data protection laws. We have a lot of lawyers at every meeting and they keep us honest. Also, the process is to follow the merchant side of the payment stream, not the consumer side. Any action that might be taken against consumers would be taken by law

enforcement. What were after is to shut down the payment account that a merchant has fraudulently opened — lets say on the credit card system.

How am I doing on time, John?

John Picarelli: ... 10 minutes left.

Cummings: OK. Great. Thank you.

Id like to take you quickly through the CyberTipline process so you get a sense of how the financial services companies interact with this. A URL is reported into the CyberTipline, as I mentioned, by a member of the general public or an Internet service provider. And that can be done by phone or via the Internet. An analyst at the National Center for Missing & Exploited Children visits the Web site and confirms that it is commercial child pornography. An undercover financial transaction is conducted by law enforcement. Right now were doing them with credit card accounts that have been contributed by some of the banks who are members. Specific details of that transaction are provided to the payment company. So an American Express or a PayPal or a Discover will get an e-mail or an alert that says, such and such a date, an undercover transaction was performed by ICE for this child pornography Web site. Please keep an eye out for when that transaction goes through. And sometimes it doesn't go through, and Ill tell you about that in a moment. When the transaction goes through the payment company isolates it and identifies the business and the location of the merchant responsible for selling the child pornography. The payment company then goes into the CyberTipline, and this is through a virtual private network, a very secure network, and only very specific companies have access to it. They amend the original report to include information on the merchant like city, state, location — or country. Also the merchant bank, city, state, country, et cetera. And other details.

The completed CyberTipline report is available to federal law enforcement for 10 days, where they can take the tip and say, Were going to add it to an ongoing investigation, or we might — they wont tell us the exact details, but they say, Were going to keep this. And if that is the case — I beg your pardon — if that is the case, if law enforcement indicates further action, the entire process stops and the financial industry is notified of a possible investigation. And then they're given instructions about what to do next as it relates to that merchant account.

In box number eight, if law enforcement declines to take the tip, the financial company is alerted and pursues the violation of association rules or merchant agreements that they would do under normal conditions when they find illegal content on their system. That basically means that they contact the merchant bank and say, You have this player on your system who is selling this contraband. Please close down that merchant account immediately. And that is what happens.

So what I just described to you is the backbone of what we do in the Financial Coalition. What we have found that it is a great form for helping each other in other ways such as disseminating trend information and other data about these Web sites. It might include price points. It might include key words that the commercial child pornography trade now uses to attract people to their sites. And so we send out these alerts, this type of information so that an AOL, a Yahoo!, a

MasterCard, everyone is able to run this information against their systems and do a better job of cleansing their systems of these businesses.

We have also published two thought-leadership pieces: a white paper and a best practices document. And we have found a lot of benefit in aligning with other industries. In this case, specifically the mobile telephone and mobile provider industry in the form of the GSMA based in London, as they try to get ahead of the mobile Internet being available on phones, and people accessing this content via phone. So more and more we are collaborating with that industry.

Now people will ask us, OK, you've been in existence since 2006, how do you know anything is happening as a result of your efforts? They ask us quite often, What about arrests? We do not measure our success by arrests because we are a civil initiative. But the things I can tell you is that the subscription prices to these Web sites has gone much, much higher. It used to be $29.95 a month. Now they can be $300, $500; sometimes we see prices as high as $1,200. Its increasingly difficult for law enforcement to do an undercover test transaction with a traditional payment tool, meaning credit cards, debit cards, PayPal, et cetera. And if its more difficult for them to do it, we've got to assume that the average consumer is having trouble as well. We've gotten very good feedback from law enforcement, and fewer commercial child pornography sites are being reported into the National Centers CyberTipline.

But this is a global problem and it requires a global solution. We have been very active in regions around the world supporting efforts in any way we can. You cant just take this U.S. model and plop it down into another country for a host of reasons. But there are things we've learned, successes we've had, challenges we've had that we are sharing with other regions of the world, and we are making great progress. You'll hear more about the Swedish Financial Coalition, and we've played a small part in that, and were very proud of that, and proud of where that group is headed. And a little while ago, a couple of weeks ago, I got back from Tokyo, where there is significant interest in the Asia-Pacific region. And some things brewing in Latin America; that's going to take a little while longer.

I very much appreciate your attention and would be happy to answer questions or further the conversation after our speakers are finished. Thank you very much.

[Applause]

Bjørn-Erik Ludvigsen, Police Superintendent, National Criminal Investigation Service, Oslo, Norway

Bjrn-Erik Ludvigsen: Good afternoon ladies and gentlemen. My name is Bjrn-Erik Ludvigsen. I [am] with the Norwegian National Police. Would be the equivalent of the FBI without the big budget and the three-piece suits.

[Laughter.]

Ludvigsen: I'm also the project manager of CIRCAMP, the COSPOL Internet-Related Child Abusive Material Project. We do a lot of aggregations, and we do it because we want people to

actually read what it says. And I will explain a little more why were called that and what other names we use.

I'm going to talk a little bit about how we came about. In 2004, OCTA, the organized crime threat assessment within Europol, tried to look into their glass bowl and see — or the crystal ball — to see what type of crimes would be a challenge for us in the future. And they usually try to see things that go cross-border or international because none of the law enforcement agencies in Europe or here in the U.S. are able to handle some of these crime types by themselves. Then they give the job to the European Police Chief Task Force, the EPCTF, and they started up these COSPOL groups. It actually stands for Comprehensive Operational Planning for the Police — no sorry, Comprehensive Operational Strategic Planning for the Police.

And they identify the different types of crime like drugs and also the distribution of child abuse material. Then they started our group. Our group was originally called the COSPOL Group on Child Pornography. One of the first things we did when we had our first meeting — and I don't mean to offend anyone because you have child pornography in your names, but we changed the name to CIRCAMP. We don't deal in child pornography; we deal in child exploitation and child abuse images and films and files. Pornography is legal in most countries. Pornography is consensual in most countries. Many people use pornography. The raping of a child is not pornography. That is our stand, anyway.

We are the project manager from Norway. You see the other countries that are members. Being a [forerunner] country means it is a country that is supposed to try out different things that we do and see if it works. And if it does, well try to translate that to other countries that are not members of this group. So we try to make kind of a standard of how to do things.

Up, sorry. By the way, were also supported by both Europol and Interpol so we have the international level covered with both communication and strategic and operational handling of information.

I'm not going to read all this to you. Our primary goal is to try to make it difficult for bad guys to make money off children being sexually abused, especially on the Internet. We also to find a common way for us to police the Internet. In our view, the Internet is just a continuation of general society and national laws should apply on the Internet. That part of the Internet which is located in my country, the Norwegian part of this network, Norwegian law applies. Its not a different dimension; its not a different country; its not a different place. Its just a bunch of computers and wires tying things together. And people are doing stuff on the Internet that needs to be policed.

We think that child abuse material has a harmful effect on society, and we would like to try to limit that as much as we can. One thing is the people like Catherine was talking about, the ones who buy child abuse material, you want to stop them but you also want to stop the people that are unwillingly being exposed to this kind of information.

We started out doing what every police Internet project does. We started going after the peer-to-peer people because its easy, because they're plentiful, because they distribute really severe child

abuse material and we know how to take those people down. We know how to secure the evidence. We know arrest them. And we know how to search their houses and their computers. This is something we did from 2004 to 2006. And then we kind of figured out, well this is something we can do by ourselves; we don't need an international group to do this. I can do this in my country, as we did actually in 2004, and make all these cases and send them around the world. In 48 hours in 2004, we generated 13,000 cases all over the world — 2,000 cases for the U.S. It is an easy way to make cases. And we decided we don't have to do that as a group.

So we went to the police chiefs and we said we want to do something else — were going to target the child abusive material that is distributed commercially, especially that on the Web. And we made a three-point action plan that we tried to follow. The first part being to block child abuse material. We have done this — were now in 2006; we had done this in Norway since 2004. And we said this is a good idea but Norway is not really the center of the earth. We need to have more people that work with us. So we suggested that would be part of the plan. The second plan would be to go after the legal element, the payment systems, like Catherine said. Identify them, tell them that they are actually being abused so that they will cut off the merchant. And the third part is try to arrest the people who actually make money off this. This is, of course, the most difficult ... most difficult part, and we haven't really succeeded much in that.

I'm going to talk about the blocking today. We want to prevent the children being abused again and again as masturbation material for adults, because that's what they use it for. They don't collect it because its like stamps. They use it to masturbate. They are sexually interested in children. The distribution is illegal in most countries that have any kind of child abuse legislation. As Catherine said, many countries do not. But those that have, distribution is always illegal, while possession may be legal still. In my country, display is illegal. If you actually go to a site looking for this kind of material willfully and repeatedly, that is a crime by itself, because you don't have to download anything anymore. Everything is online and with the speed we have on our Internet connections, you don't have to possess anything in the ordinary sense of the word.

And by reducing the access to child abuse material we think that we can reduce the market. Take away the customer, there is no need to produce and offer as much material. This is, you know, capitalism at its best and its worst. If there's a need, there will be a supply. Take away the demand for child abuse material. And we do it by targeting the whole chain: the contents, the links sites, the payment sites, anything we can see is a link in the commercial distribution of child abuse material.

And we wanted also to raise the awareness in the population — both the ones that look for it and the ones that are accidentally exposed to it. And with this I'm making another aggregation, of course. And instead of calling it the child pornography filter, we call it the child sexual abuse anti-distribution filter because that's what it does. It limits the distribution of child abusive material. And this is how it works. Well, this is really simplified, but you'll get the idea. This is kind of like how the Internet works. Most of you, if you ever spend time on the Internet know that the Internet does not work with letters. It doesn't work with words, it works with numbers and IP addresses. So when you type something into your browser, it needs to be translated to an IP address so that your computer — your browser knows where the content you're looking for is.

And it does this by going to a DNS server, looking up who is responsible for childporn.com, in this case. And the DNS will say its IP address this and that. And your browser will connect directly to that server. It may be in Russia, it may be in U.S. You don't know. And if you punch child pornography or childporn.com into your browser, you will get childporn.com. Of course, I couldn't show you how this site looks, as I didn't want to spend time in your jails.

[Laughter.]

Ludvigsen: You have really good laws against the people you arrest for this crime, really good laws. Unfortunately, of course, you don't arrest as many as I would like but when you get them you actually give them a good sentencing, which I cant say about my own country unfortunately. Well, you type in what you want, you get what you want. This could be your online newspaper, this could be children being raped. By introducing a new layer where you will still punch in what you want — the child pornography or the childpornographysite.com — you will check it against a list of domains that we have given to the ISP. All of the domains on this list have been checked by the police. The contents have been seized. We have downloaded everything. Everything is traced and saved and secured. And then we say that the images or the content on this site is in breach of our laws. Our national legislation says that this is illegal to distribute. Then we will put it on this list. The ISP will check it against that list when you try to access the site and if its on the list, you will get this site instead. Instead of the child abusive material you saw before, you will get this stop page. And we will put — this is the Norwegian one, by the way. And I hope you can read what it says.

We don't say that you have been trying to access child abuse material, but we say your browser has been trying to access child abuse material.

[Laughter.]

Ludvigsen: So were not pointing any fingers here. And the reason for this is that, quite frankly, some people are not that intelligent when they are on the Internet. Some people are mindlessly surfing. Some people are clicking everything that looks like a link, even if they get it in an e-mail. Some people surf borderline pornography. They look ... they'll go for the teen sites with the 18 and 19 year olds. And they're very quickly linked to sites that contain children. So its not always a willing act to end up on one of these child abuse material sites. That's why we said your browser. In addition, there's Trojans and viruses and all kinds of bad things that will redirect you to sites that you don't want to go.

In addition we say that we don't trace anything. We don't know who you are. We don't make any cases from the people that end up getting this site or this page. This is just a pure preventive measure against the distribution of child abuse material. And in my view, prevention is the most noble of all police work.

Also we have information about the operation of [indistinguishable], the CIRCAMP group. Just to tell people, this is not something we only do in Norway. This is something we do together because, as you all know, the Internet is not limited to one country or one continent.

These are the countries that are in CIRCAMP that run the blocking system right now. And what happens when I find a new site, I download and [indistinguishable]; I do all the things the police should do when they secure evidence, and I will share it with all these guys, so they don't have to go looking for these kinds of sites on the Internet. They will just get it from me, check it according to their own legislation. If its illegal in Finland, then they will just add it to their local list of sites that I've blocked. So even though we share all the material, all of this will look different because we all have different laws. In my country, for instance, almost everything is illegal. Even computer-generated, drawn pictures are illegal if it depicts a child.

These are countries outside of our little group that we also work with. So New Zealand on the other side of the world and Switzerland, its a European country, but they're not in the European Union. And also there's the United Kingdom that has a similar system driven by the Internet Watch Foundation, which is a non-governmental organization, and is financed by the Internet industry.

These are just some examples of stop pages. This is the Swiss one, Danish, Finnish, Italian, New Zealand's — New Zealand's The Swedish one, which I think Per-Ake will tell you about. And the one from Malta. And this is very important people, because this is not the Holy Grail of child abuse material fighting. This doesn't stop any of the child abuse material from being produced or from being distributed to other countries that are not members of this.

How am I on time?

[Inaudible]

Ludvigsen: Oh. So this is something we do in addition to ordinary police work, not instead of. So you cant introduce blocking and say, Oh, well problem solved. I don't have to do anymore. Then your work really starts. But then you will have a huge chunk of work that you don't have to do. Again, if you are able to limit the access to that material.

This is just information about our project. You can find it on the Europol page. This is on the Interpol page, on the THB, the Trafficking and Human Being Web site for Interpol. We also have our own Web site. Its on CIRCAMP.eu, where well have — its kind of limited thus far, but we will have more information on that site about terminology, which I think is very important. And a little bit about how we think when we try to limit this kind of material being distributed.

Our plan ahead is to continue the work that we do now until 2010. That doesn't mean that were going to quit doing this in 2010, but CIRCAMP as a group will probably have another aim. And the countries that have the blocking will continue to do that on their own account. We plan to make a worst-of list of domains. And a worst-of would be — because now, the list we have in Norway is based on Norwegian legislation. In Sweden, its Swedish, et cetera. But there are a number of countries where we don't have any contacts with the police. The police don't have the people, the knowledge, the interest to do so. And we plan to make a worst-of list of sites that would be illegal anywhere. That means it will be with children that are younger than 13. It will be the most horrific abuse of children, or very particular sexual focus on any of the images on that site. It has to be a real child, for instance. Not computer-generated, which is legal in some

countries. And we plan to distribute this through the Interpol National Central Bureaus, because every one of the 187, was it, Catherine? Yeah. Every one of the 187 countries had a contact bureau for Interpol, and we need to spread this list of worst-of sites to all those contact points and then the ISPs so the access service providers can contact the Interpol police office and get access to the group and implement it, based on their terms of service, their ethical standpoint or their policy. And we are often contacted by Internet service providers that want to do something good for the Internet, want to make the Internet a better place, but have no one to turn to because the police in that country are unwilling or unable to provide a list according to that country's legislation. The list is something that we will do.

We will also continue our cooperation with Germany, for instance, which actually wrote contracts with six other larger-sized ISPs in April that will start blocking very soon. It is very important for us because it is a big country, or by European standards its a big country with 90 million people. And we will work with law enforcement in any country — any country in the world, although we are a European project.

To sum up the whole thing, we are a very sharing group, but we will only share with law enforcement when it comes to child abuse material because we look at child abuse material as evidence of a crime. Its a picture that usually the perpetrator himself has taken, and it shows the crime scene, and it shows at least parts of the perpetrator, and it will show the victim. And all these things are important things for the police to use to try to identify the child and try to stop the abuse. So that's why we will only share child abuse material with the police. Well happily work with any NGO on other things, but we will not share the images with them. And we will share every smart thing that we've ever thought, any software that we ever made and any contract that we have ever written with any ISP to bring people up to speed much quicker than we were when we first started.

The benefits are that its very cheap. This is — some people will say differently, and especially some ISPs will say differently, but this is actually pretty simple, simple readdressing on the Internet and they do this every day. This is not brain surgery in any way. We use ordinary software, ordinary techniques, off-the-shelf things that you can buy. There's nothing really peculiar about the operation. I know Per-Ake will talk a little about a special software that we have, but you don't really need that.

It is very effective. Compared to what you invest in this system and what you get out, its very, very effective. I'm not going to give you so much numbers — actually I can see from my country, but we have very strict rules, we have about one display of this stop page that I showed you before per 300 people in my country per day. So we have like 15 to 18,000 displays of our stop page on a 4.7 million population. So it is quite a number of people that are actually looking for, or accidentally end up on child abusive sites.

And we believe that it is preventive. It will give people looking for this willingly, a kind of a heads up in saying, What are you doing? It will give people that are swimming in murky waters kind of a way to step back, age-wise, when it comes to the pornography that they use. And it will give the people that are not-so-knowledgeable when they surf the Internet a way not to be exposed to children being raped, which they easily can be.

That is the presentation that I had planned, and Ill be happy to answer any questions when the Q and A starts after Per-Ake. Thank you.

Per-Ake Wecksell, Detective Inspector, Swedish National Criminal Police, Stockholm, Sweden

Per-Ake Wecksell: Ill have to put this down again. My name is Per-Ake Wecksell, but you can call me, as Bjrn, Pela. I work for the Swedish National Criminal Police, our anti-crime section on the child protection team. I come from Sweden, the land of IKEA, Volvo, ABBA ...

[Laughter.]

Wecksell: ABSOLUT Vodka, and Greta Garbo.

[Laughter.]

Wecksell: I'm going to talk about the collaboration with the industry in this matter, about challenges that we have met, and finally short about the Swedish Financial Coalition.

As I will talk on a national level now, instead of the CIRCAMP level, I will tell you the Swedish matter. And it all started as an initiative from Norway and Bjrn-Eriks team. It was their criminal investigation team who taught us, and we gathered together the representatives from law enforcement and industry to discuss whether we should have this blocking system in Sweden or not. And suddenly, an agreement was made and a contract was written between several Swedish Internet service providers and the Swedish National Criminal Police.

And this collaboration between the police and the Internet service providers is completely built on a volatile basis and is the crime preventive work. As Bjrn-Erik told, in Norway its forbidden to watch these sites of child abusive images but its not in Sweden. There is a law going to be, but its not still written. So, however, its not forbidden, but it is forbidden to be in possession or distribute this kind of material.

This is crime preventive work. Today we have a collaboration, contracted 16 ISPs in this blocking solution. And they have a coverage of about 80 to 90 percent of the Swedish Internet users. And new contracts are assigned, on the way, and now we are talking to the local networks on the cities around Sweden.

However, one of the largest Swedish ISPs didn't want to participate in this collaboration from the beginning. I don't want to mention their name because its audio taped here, but ...

[Laughter.]

Wecksell: The biggest Swedish newspaper told about it. A poll was made and a huge majority of the Swedish population said they should block — they should contribute to this work against this matter. And the criticism was too difficult for the company, and the next day, after the article

was published, they told us that they want to be in the collaboration. But I'm sure that you already had read it.

[Laughter.]

Wecksell: Yeah? You have recently heard Mr. Bjrn-Erik Ludvigsen from Norway talk about how the blocking of a Web site actually works. I'm not going to repeat that. However, we, the Swedish NCPs, receive data information from [the] public regarding child abusive images on Internet sites. We get referrals from ISPs. We get information from the other European network, the CIRCAMP network, and from the EPCOT, the Swedish non-governmental organization, EPCOT's hotline. Also, we got these URLs that were found on computers which were seized all around Sweden during investigations. The role of the law enforcement is to collect those reported URLs and to review and investigate and make a judgment if these Web sites are legal or not, regarding Swedish law. If they are considered illegal, they will be blocked. We create and send a text file to the providers that will see that the sites will be blocked.

Bjrn-Erik also told you about a special program, and here is the program we use to make life a little easier when we deal with this matter. Its created by the Danish police. And we put in a text link for all the information we got, and it [indistinguishable] to have it on the domain level, as you can see. And we click on it and check all these sites, and if we consider them illegal we save the sites and we give them a red flag, as in blocked. If its not illegal, we give them a green flag. You can see, you have this flag here from some country. In this case, its just one country's flag here, but otherwise it will show all the countries where the Web sites belong to. This is a good instrument that we use. The role of the Internet service providers is simply to implement the blocking list or the DNS servers. They have to provide statistic referrals and implement the stop page, which you recently have seen. As Bjrn-Erik told you it says, Your Web browser has tried to contact an Internet Web site, and what penal code is used, in this case, Chapter 16. And where to turn to if one has some complaints to do.

And this stop site is shown double as many times as the Norwegian — 1,000 times per day because we are double the population in Sweden regarding Norway — compared to Norway.

I will show you our written agreement. I will not.

[Laughter.]

Wecksell: I will. OK. This is signed by the chief of the National Criminal Police and the chief of the Internet service provider. I will just go through it very quickly. You see that the corporation is aimed at restricting access to, and circulation of, descriptions of children in pornographic pictures on the Internet, as well as in that way preventing children from being sexually abused. It says about NCPs commitments, the Internet service providers commitments. I hope you all manage to read this now. And it states that the parties shall meet at least once a year, in addition to that when necessary to elevate the corporation. I can say that we meet three to four times a year. The agreement can be cancelled by one of the parties with immediate effect. Now I think I have this in the slides, so you can read it more carefully if you want, later.

OK. So is everything going smooth and nice with this? Yes, it is. But we have a few small challenges. The Swedish Post and Telecom Agency monitors the electronic communications and postal sectors in Sweden. They have been with this meeting for two years, and after two years they came to the meeting and brought up the issue of the agreements between customers and ISP approval to regulate Internet traffic carrying child abusive material. Lack of such regulation could lead to imprisonment for the responsible person at the Internet service providers. I can tell you that participants got their coffee stuck in their throats. This person from the Swedish Post and Telecom Agency, he really liked that, so he told them time and time again about this chance to go to jail if they have no regulation. But they went home and checked their agreements between them and the customers and everything was written down and good.

Another challenge is, OK, you are blocking child abusive images today, but what will the next step be? Bestiality or something else? Is this the first step in blocking the whole Internet or what? Norway started early 2004 and we started 2005 and it will be nothing else. It will stay with child abusive images. I can tell you for that by our countries. I'm sure that Bjrn-Erik will agree with me.

By the end of 2008 we made a new agreement between us and the ISPs for the enrollment of referrals, the page before coming to the Web site, with the stop sign. Some other adjustments were also made. For example, to involve non-commercial pages in the agreement. But it proved controversial to make changes in the agreement. Now were talking about [indistinguishable] and slippery slope again. Two of the largest Internet Service Providers, one that you remember from the earlier slide, and another said they didn't want to help the police with the investigation. And they said that we could do it by ourselves. The investigation, giving us the site, the referrals. I don't know about that, but ... finally we have these meetings and they signed a new agreement. But a response came quickly from ...

[Laughter.]

Wecksell: The first opportunity to give us referrals, and we expected tens of thousands of referrals. We got 50 — five, zero — because the agreement says nothing about how many referrals we were supposed to get.

Finally, the last challenge was BitTorrent, Pirate Bay. Anybody heard about Pirate Bay? You know about BitTorrent? We received information that a lot of the worlds largest BitTorrent tracker had files that contained child abusive images and material. Files, it was films and pictures. BitTorrent is a file sharing protocol that enables file transfers. Pirate Bay offers — uses the latest Hollywood movies, the latest games, or whatever the latest books, e-books. And the tips, information about child abusive images and material on Pirate Bay increased, so we had to decide whether this site was going to be blocked or not. We called a meeting, in a very high level, international police, Swedish National Police, and it was decided that if they will not take away this abusive material over the weekend, they will be blocked. So I sent out this information to the Internet Service Providers, just to prepare them for some Internet attacks, who could be. And I sent it on a secure way to those responsible on the ISPs. It took — then I went to my holiday. I go down to the south of Sweden to meet my son, and I just come one hours drive when the telephone called. Hi, its Pirate Bay. And the name of the guy. Are you going to block Pirate

Bay? And directly after we hang up, the Aftonbladet, the Swedish biggest newspaper called. And after that, a lawyer for one of the biggest ISPs called me.

[Laughter.]

Wecksell: Are you going to block Pirate Bay? The circus started. It was a big fuss in the mass media, and we received a lot of complaints by mail. People said, This is going to be the new China. We want these Torrents to live. Keep away from Pirate Bay. Three major Swedish Web sites were hacked, and they put in our stop page instead of the material who belongs to it. One of the Web sites was from one of the most popular soccer teams in Sweden, and their supporters were crazy about us. People thought we were the ones that blocked the Web site. And the circus went on. However, on Monday morning, I went to work. The team which I worked with checked out the Pirate Bay, and the child abusive material was gone. However, the turbulence continued a couple of weeks. But it led to something good. We [had] shaken the Pirate Bay a little bit and now we have a good collaboration with them, and they even put our e-mail address on their Web site.

OK. Results in the end of this blocking. We can see that the child abusive material is less available in Sweden. ISPs take more responsibility. The Swedish public is very much positive about this work. I can show you that we got mail every day, people thanking us. And we also get telephone calls by people who run into these sites, come to the stop page, and they call us and say, What is going to happen now? Are you going to come to get me?

[Laughter.]

So. Yeah. But were not.

This is a political, very well accepted method. And I will say this has a large preventive effect. So, the next step. Like Catherine talked about, there was a Financial Coalition going on here in the United States, and the next stop for us has now been taken. The nongovernment organization, EPCOT has looked at the Financial Coalition in the USA. And I would like to thank you, Catherine, for all the help to bring the Financial Coalition to Sweden. We have a collaboration now between Skandiabanken and the Swedish National Criminal Police. And it differs some from the U.S. Financial Coalition. In Sweden we have no domains or servers that are hosted here, and if we have, we will start an investigation, at least we don't find them. What we do is that we receive a number of accounts from the bank with complete information to make purchases on the Internet, like Catherine recently told you about. So we do it, something like the Financial Coalition in the States do, but not really like that. We have a cooperation between the banks, the Visa, the MasterCard's, and the aim is to prevent and obstruct payments for child abusive material through the financial system.

Yes. I think I will stop there. And here is my address if you want to e-mail me, and I will be glad to — thank you for your attention and I will take questions later. Thank you.

June 2009

Moderator: John Picarelli, Social Science Analyst, National Institute of Justice Panelists:

- Catherine J. Cummings, Executive Director, Financial Coalition Against Child Pornography, International Center for Missing and Exploited Children
- Bjørn-Erik Ludvigsen, Police Superintendent, National Criminal Investigation Service, Oslo, Norway
- Per-Ake Wecksell, Detective Inspector, Swedish National Criminal Police, Stockholm, Sweden

Close this window

NIJ's Multimedia Page | **NIJ's Home Page**

Date Modified: April 5, 2010