FEDERAL TRADE COMMISSION

WORKSHOP:

PARTNERSHIPS AGAINST CROSS-BORDER FRAUD

THURSDAY, FEBRUARY 20, 2003

FEDERAL TRADE COMMISSION
6TH AND PENNSYLVANIA AVENUE, N.W.
WASHINGTON, D.C.

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025

TABLE OF CONTENTS

P R O C E E D I N G S

- - - - - -

MR. STEVENSON: We're ready to get started. We seem to have lost one panelist in the snow. We are going to proceed ahead.

COMMISSIONER THOMPSON: It's a conspiracy. If we don't like you, we lose you in the snow.

Good morning, you all. Thank you very much for coming to the FTC for our second day on our partnerships against cross-border fraud workshop. Now, I know there are a lot of you who have come from very long distances to be here and participate. I'm specifically mentioning our folks from the customs service and -- no, some of our foreign guests from Australia and the UK and, yes, even Canada, where they think the snow that we've had is just like a little blip.

Well, thank you very much for coming. Now, yesterday, we heard some very interesting discussion, especially about cross-border fraud trends in the financial services industry, and heard a little bit about the experiences in financial services in combatting cross-border fraud. Today, we're going to hear some other interesting information from people who are involved with commercial mail, people involved in industry self-regulation and in the more high-tech

industries of the Internet. We'll also hear after lunch from the domain registration authorities, one I'm particularly interested in.

So, now, yesterday I talked a little bit about some of the real opportunities that we have here in combatting cross-border fraud, but also the recognition that neither government nor businesses, nor consumers, alone, could find solutions to fraud that takes place on a global basis. It's an opportunity for us to set aside our usual suspicions about how different branches of the world operate and to recognize in order to set the right course for the future, and that future is something we all have an interest in, that we have to work more cooperatively and to recognize that each of us have a role in shaping what future policy is.

So, I'm not going to delay too long, because I know that we want to get to the panels, and to hear what they have to say. So, on that note, I welcome you all here, and I again want to give a special thanks to the staff who put this together, the folks in the International Consumer Protection, who have worked really hard to arrange the snow, and everybody who has especially brought materials here and left it out on the table in hopes that they won't have to carry them home.

So, thank you very much for coming. And, now,

there's just one point that I do want to raise as part of my prerogative, is this: I would like to see this as a starting point and not an ending point. I think that we've spent a long time, each of us, working in our various fields talking about, gee, wouldn't it be nice if we found more formal ways of cooperating with each other to solve these problems.

It is my hope, whether it's on a one-on-one basis by the people sitting in this room, or by looking at the categories of subjects that we've talked about today and tomorrow, yesterday and today, that we can sit down and have a more formal relationship, and hopefully, perhaps, have more of these workshops, either here sponsored by the FTC, or outside of the FTC where we can work on solutions and identifying new problems as they arise.

So, that's the challenge that I have for all of you, to make this last beyond what we've gone through in two days, but to make it more meaningful for consumers and businesses, and, yes, even us in government, because we're here to help you. Thank you very much.

MS. FEUER: Great, I would like to get started now with our first panel, so if the panelists can come up and take their seats by their placards, that would be great.

Before we get started, I just want to apologize for leaving my cell phone on. We are missing one panelist, Charmaine Fennie, who I believe is traveling on the red eye from Seattle. So, unfortunately, we are going to get started without her, and there is a gap, but if my cell phone rings, I apologize, because I left my number for her to call.

So, with that, good morning, I'm Stacy Feuer, Legal Advisor for International Consumer Protection here at the FTC. During the last panel yesterday, we focused on payment systems, a type of legitimate business, or I should say businesses that are often used by cross-border fraud operators to facilitate frauds, mainly to get money from victims. Today we're going to look at two other types of legitimate businesses that are often used by fraud operators for the same purposes, as well as for other incidental matters in fraud schemes.

To discuss this, I am pleased to welcome, and I'll do this alphabetically, so if you want to just raise your hand, Alan Armstrong, who is a long-time major franchisee for MailBoxes Etc., and he is responsible for the Washington metropolitan area. He is here representing MBE, both at the regional and corporate level.

Also, Lee Hollis, who is the General Manager for Enforcement Coordination at the Australian Competition and Consumer Commission. Robin Landis, next to me, the Program Manager for Telemarketing Fraud with the U.S. Customs Service. He recently returned to DC after working with our law enforcement counterparts across the border for the past year or so, through Project Colt in Montreal.

Larry Maxwell -- sorry, I skipped Andy Lynn, Director of Marketing and International Property Law at FedEx. In that capacity, Andy works with the security, revenue and IT units at FedEx to detect and prevent fraudulent transactions. And last but not least, Larry Maxwell, the Inspector in Charge of the Fraud, Child Exploitation, and Asset Forfeiture Group for the Postal Inspection Service.

What I would like to do with this panel, as we did yesterday afternoon, is throw out a few questions, first about opening matters such as current issues and trends affecting the use of CMRAs and courier services in the cross-border fraud arena, and then halfway through, move on to possible mechanisms for enhanced cooperation between law enforcement agencies, including the three of us who are sitting here, Customs, the U.S. Postal Inspection Service and the FTC, and the private

sector.

What I would like to do is keep this discussion interactive. So, while I'll address some of my questions to particular panelists, if you want to respond and weigh in on somebody's comments or a question I have asked, just raise your table tent and I will recognize you.

So, I am going to start with Robin, since he is sitting right next to me, and ask, what are the main challenges you see for law enforcement arising out of the use of commercial receiving mail agencies and courier services in fraudulent cross-border telemarketing schemes?

MR. LANDIS: Well, thank you, Stacy, I appreciate coming here to talk to you about telemarketing fraud.

The U.S. Customs Service believes that telemarketing fraud is a big problem. I spent three years up in Montreal just doing telemarketing, and we just opened an office with three agents working in Montreal, Toronto, and Vancouver that's trying to address this problem. And I would like to kind of explain to you how it really works.

Now, would you be surprised if I told you that telemarketing out of Canada is organized crime? It's

organized crime. It is organized crime. The proceeds that they're receiving from this telemarketing fraud, and we estimate just in Montreal alone is $200 million, just Montreal. These proceeds are being used to buy narcotics, to fund drug operations, the smuggling of guns, and prostitution. We have documented this. It is organized crime.

It's set up basically in a four-part organization. They have a leader, a captain, and they have lieutenants. How is it broken down? Well, you have a lieutenant that's in charge of leads. Leads are the victims' telephone numbers. That is very, very sought after. You have another lieutenant who is in charge of the boiler rooms, or the telemarketers. When I say boiler rooms, you probably think of a room that they rent in a business, it's not that anymore. It could be five, six, seven people sitting in cars in a parking lot of a mall with cell phones, calling the victims with their lead sheets. Or it could be a hotel room where they rent it for 24 hours. They move very fast.

So, the boiler room has really changed to a mobile location. It's all in charge by one individual, a lieutenant.

The third lieutenant would be in charge of the

money laundering. You have the leads, the telemarketers, then they have to get the money. So, they have a person in charge of nothing but pertaining to money.

And a fourth lieutenant who is in charge of security. And what I mean by security, they enforce and keep the organization together. They do not want the telemarketers to steal any of the leads, they want to make sure that the leads are brought in timely, and it just keeps the organization together. Most of the security people are street gang members. Very violent.

How do we attack this? We want to attack it by prevention, disruption, and prosecution. When I talk to you about leads, that is probably the most important thing that they look at. Every search warrant that we've done in Montreal, we always found the original leads sheets. A lead sheet is a mailing of a sweepstakes somewhere to somebody in the United States asking them to enter a contest and put their phone number on it. We are finding the original sweepstakes in Montreal from these telemarketers. They're either mailed from outside the United States or within the United States to the victims who respond.

How do we prevent this? Well, we have executed some search warrants in the United States to go after

the leads brokers. The sweepstakes entries. We want to prevent it because we think that's the key to the telemarketers. If they don't have the phone numbers, they're not going to call the victims. We want to prevent the person of responding to the calls, so prevent the mailings, prevent the telephone calls, and then prevent the victim from sending the money. That's our prevention strategy in telemarketing.

Disruption: What I mean by disruption, we want to seize the mailings, shut down the phone lines, or seize the money coming from the United States to the foreign country.

In one case that I worked starting in '92, one telemarketing organization out of Canada had three boiler rooms. Their telephone bill was over $1 million a month with 1,000 telemarketers calling to the United States seven days a week, 16 hours a day. In the indictment we had, we documented $118 million in one year.

We're also shutting down phone lines and we're also seizing mail that's coming into or going out of the United States. We're also conducting a lot of prosecutions lately, with the U.S. Attorney's Office from mailers, printers, who are aiding and abetting, knowingly. The telemarketers that are doing the

telephone calls in Canada, and elsewhere, and also the money launderers, which include money transmitters, bank-to-bank wire transfers, and also individuals who are operating drop sites.

Working with the mail receivers or the express couriers, last year, just in Montreal, we intercepted and seized over $1 million cash going to telemarketers in Montreal. Under our program, we seize it, we return the money back to the individuals. U.S. Customs agents actually go to the victim in the United States, return the money to them, and interview them to see why they were victimized, what was the statements made to them, what were the promises, and why they sent it.

Just one year operation in Montreal, we have documented over 1,500 drop sites where mail is going to them from telemarketers.

MS. FEUER: Robin, thank you. So, yesterday we talked about money going to a wire transfer through a debit card through ACH Debits, but what you're saying to me it sounds like Customs Service is still seizing lots of money that the victims are sending that is making its way from the victims' pockets to the telemarketers by the mail and express mailing couriers.

MR. LANDIS: Correct. A lot of it is cash, a

lot of it is cashier's checks.

MS. FEUER: And that's interesting, because it does seem consistent with some of the new statistics that we're releasing that checks are still a big payment method in these schemes.

I'm wondering, Larry, whether you're seeing the same types of things, and if you could focus in part on obviously the Postal Inspection Service viewpoint how CMRAs are used and what kinds of trends you're seeing in connection with telemarketing fraud and Internet fraud as well.

MR. MAXWELL: Sure. First, Stacy, I just want to thank the Commissioner and FTC for hosting us and inviting me and my agency and our friends here from the other agencies.

Everything Robin just mentioned is dead on point, accurate. As he said, he spent time up in Montreal. We have an inspector assigned to Montreal and we are exploring expanding our role up there. We've been up there for several years now. We also have an inspector, two inspectors assigned to the Partnership Alliance in Toronto with FTC, and we're starting a new operation now out in Vancouver and the western part of the country.

As Robin mentioned, organized crime is a real

factor in Montreal, and telemarketing is the big focus there for us. If you go to Toronto, one of our biggest concerns there has been the advanced fee schemes, but there's a variety of other types of frauds we do see. You get out west, of great concern to me, being a representative of the Postal Service here, is the lottery, we have a preponderance of lottery schemes coming in. I hear this from the Canadian authorities and I hear this from consumer agencies, I hear this from FTC and Department of Justice.

So, we kind of have a little different hydra, if you will, in terms of the types of crimes, in terms of the use of commercial mail receiving agencies. I left a brochure out -- it's not a brochure, it's a couple of pages that the Postal Service and the Inspection Service put out a few years ago when we enhanced our regulatory provisions guiding commercial mail receiving agencies. And essentially, it lays out the facts for you and it's pretty current.

There are a few modifications that it doesn't mention that I can clarify later if you have any questions, but primarily, what we did was, and this goes in a chapter No Good Deed Goes Unpunished. We heard for years from law enforcement, both in Canada and here in the States, that commercial mail receiving agencies were

becoming a haven for criminals. Well, we only had anecdotal information. We only had agents telling us this. None of our databases captured this information, ours or others.

But we tried to proceed in enforcing new regulations and met with a very logical reaction from the industry. You know, you're basically taking a shotgun to a canary here. And we looked at it and decided the best course was to meet with them and work out reasonable accommodations that fit both sides.

We recognized we couldn't force feed our thoughts on anyone based on no empirical data to back us up. So, we agreed to modify our data mechanisms to capture those statistics so we would have a better clue and also provide some intelligence for future investigations and trend analysis. But lacking that, we worked on what I would call a common sense parameter.

Oftentimes in telemarketing schemes, both within the States, for instance in New York, where I get my experience from, you would have boiler rooms operating very temporarily, using phones, and they would use commercial mail receiving drops. Sometimes they would even use a post office box, but post office boxes had a little more direct contact with the Post Office, so there was a reluctance to use that on their part.

They could use pretty much anything to describe the address, as many of you probably are very familiar with, you could use suite 24, and to a potential victim customer, could look at that and say it sounds like a legitimate concern and mail it off thinking it goes to a nice corporate building somewhere, where in reality it went to a small mail drop place and the person would come in in anonymity, sometimes sending someone else down to pick it up.

There were requirements on the books that frankly the Postal Service didn't do a good job at enforcing at this time, and that was a form required. It's an application for delivery of mail through an agent. It's a 1583, so we will feel comfortable with government forms. There's two forms. There's one form the CMRA operator fills out which authorizes them to be a CMRA, and that's a little bit more comprehensive in terms of information required.

The second, which is the CMRA boxholder, fills out an application the same way. What we did in the new regulations, just in a nutshell is we enhanced the identification requirements and the validation of those requirements. So, the postmaster validates the CMRA, the CMRA owner/operator would validate their customers. And on a quarterly basis, provides that information to

local post offices, the current list. So, we have a listing of actually who we deliver mail to.

Does the Postal Service compile lists of private information, social security number, addresses? No, we do not. And as a law enforcement officer, I would love to have that information, because it would make my job a lot easier, but in a democracy, there are groups that feel that's an intrusion of privacy, and we have to respect that.

I was part of a side working group dealing with the abused spouse organizations, and they had some major concerns about releasing this information, even to law enforcement, without court orders. So, we restricted a lot of that information based on our recognition that there are people who could get hurt in this process for us. So, that is a big obstacle we have faced.

We have mechanisms in place now which appear to be working. Recently, I ran the statistics, which does not show a dramatic usage of CMRAs to my surprise, but part of that comes, it's like the chicken and the egg. I mean, we implemented these new regulations, which eliminated mailers from using terms like suite or some other designation for an office, and they had to use two designations, they had to use either the term PMB, for private mailbox, similar to post office box, and that

seemed like a good catch, we had a nice comparison. However, some people did push back on that, and they felt they wanted one other alternative, because they felt PMB was too restrictive.

And, again, you're dealing with a lot of legitimate businesses that have needs and want to change and have image and branding and so forth. So, we gave them the pound sign, the numeric pound sign symbol, they could use that, or PMB. And that may have, for those honest operators out there, those mailers, that may have decreased some of the use of the CMRAs, in the United States.

There are commercial mail receiving agencies, of course, around the globe. We have worked, as I'm sure Robin has, and others here, with Canadian counterparts. And just like you would a victim on the street or a witness on the street, some are very cooperative and helpful, even when they don't have to be, and then others basically tell us to take a hike.

So, we have no legal jurisdiction to enforce them. The Canada Post Institution, which is the U.S. Postal Service counterpart, they do not have requirements on registering commercial mail receiving agencies, to my knowledge, unless that's changed very recently, and I don't believe it has.

Again, I don't know if their thinking is to enforce such regulatory change up there, but I think they saw what we went through and probably thought better of it. But they may at some point. And I think it is good to know your customer, who you deliver to, and it protects a lot of people, and it protects the Post Office. We deliver to a lot of people. And that creates another major obstacle.

Again, this information is private information, people like to protect their identity, they do like to protect their personal privacy for a lot of reasons. And in some instances are very open out there. But we have to respect both parties. So, that does present a challenge.

My concern goes even further in dealing with the cross-border issue. It's been a great opportunity for U.S. law enforcement and Canadian law enforcement to work together to iron out a lot of these kinks that come from two very friendly nations that speak mostly the same language and share a lot of the same institutions and laws. What's happening is, as all of you are aware, and it's a big focus of Hugh Stevenson and his group, is the emergence of international fraud and crimes and how we are going to deal with that in the coming decades.

That's a concern. I mean, over the years, we've had trouble keeping the genie in the bottle on our own domestic crimes and now we're looking at victimization from outside our parameters. And I think using the data and intelligence is a great asset for us. If we can show trends. For example, very clearly, we're seeing most of the victims coming from the lottery schemes and the operations coming from western Canada, are in the Southern California/Arizona area. It pops out at you on a map when you run some of that data and it's very helpful to use FTC data or our own data, data provided by the Canadians. And that's helpful.

MS. FEUER: Thanks. And, Larry, one follow-up question before we move on. It's good to hear that CMRAs are being used less in these schemes. I'm wondering, though, about the phenomenon that we sometimes hear in our investigations is somebody using a U.S. address at a commercial mail receiving agency and then having that mail forwarded on to Canada or some other place. Does your data pick any of that up?

MR. MAXWELL: No, that is a lacking portion. What happens is the Postal Service, although now I think we're much better off in our working relationships with the commercial mail receiving agency industry. We have a lot more contacts, there's a lot more communication,

if you will. And as I said, the vast majority are legitimate users of that service and it's a very valuable service. However, we do not regulate. We can regulate our requirements to deliver mail to that agency, but we can't regulate the users and we can't regulate the industry and what they choose to do.

MS. FEUER: Right.

MR. MAXWELL: So they can forward it on. We can't require records of that. Our hope there is cooperation from the agency manager that maybe would alert us to some kind of suspicion. Again, you know, it's sort of a dichotomy there, because they have customers, they want to preserve their privacy.

We also rely on Customs, our Customs, Canadian Customs. I'm looking at ways now, it's interesting, you were talking about forwarding the mail out, Robin was talking about a conversation we had earlier, too, was what interests me is that to get around the border search now, what they do is mail into the United States or actually have the printing done in the United States. Robin mentioned that they shut down some printers. That's probably one of the better strategies right now to use is to look at what's happening here in the United States that we can control.

You know, are they printing, producing, mailing,

distributing here? If they're forwarding it, that's a different animal there.

MS. FEUER: Right. Let me turn to Alan Armstrong, who is --

MR. ARMSTRONG: Do I get my chance now?

MS. FEUER: Yes, he was our lone CMRA representative because unfortunately Charmaine Fennie has not made it. But, Alan, let me ask you the flip side, because you and I have talked about the fact that CMRAs are used for a variety of scams, including consumer scams, but we talked a little bit about what's being done by MBE in that area. So, if you could expound on that for us.

MR. ARMSTRONG: I mean, there was a lot of things that were covered by Larry, and I know that -- and I agree with a tremendous amount of them. I think I would like to say to begin with that cooperation, particularly at the local level, between our individual stores and centers, and I don't mean to speak for the entire industry, I can speak for MBE, but I think I'm pretty comfortable in saying that it's this way with the other franchises and also with the independents that Charmaine represents.

Going at it another way, I think at the local level to work with the Postal Service, the Secret

Service, the FBI, and God knows how many other people we see kind of come into our facilities over the years.

I just want to say that those of you who read my background, I'm an area franchisee from MailBoxes Etc., but 17 years ago when I got started with MailBoxes Etc., I was an individual store owner and I had a couple of stores. So, I kind of lived all this, and the customers coming in and the problems and the concerns and dealing with the Postal Service and all these other folks. And it's been a lot of change over the years. And I think we've learned an awful lot about each other and how we can work together.

So, I think there has been a lot in that regard. I would mention that there are sometimes conflicting regulations as it relates to the pressures on the individual CMRA in terms of trying to work with the authorities, whether they be the Postal Service or the FBI, the Secret Service, in terms of trying to want to help, and at the same time being constrained by Privacy Act regulations and other sorts of things where you can find yourself on the chopping block, so to speak, your head, no matter what you do.

And to be quite truthful, I suspect in large measure that our individual franchisees probably go out on the line in terms of trying to help the Postal

Service and the FBI and the Secret Service, probably beyond what they probably should in terms of the legal perspective. And I shared that with Stacy and I say that -- is somebody taking this down? I see somebody over there is doing that. So, can we strike that last part? [Laughter].

But I think that's a reality of the situation. Our guys are local guys, they want to help, they want to be -- they want to make -- do the right thing. I mean, they're citizens, and they want to do the right thing. And a lot of our guys are actually the people that tip off the Postal Service as to things that are going on. And we've received a lot of kudos in that respect.

MS. FEUER: Are there particular things -- when you say that your CMRA MBE, in this case -- franchisees are aware of that caused them to make that call? Are there trends that you are seeing with respect to the types of scams that you are seeing run through CMRAs?

MR. ARMSTRONG: Well, the scams have changed over the years. When there's a crook, they're always trying to think of a different way to use whatever they can find to make a quick buck or two. But I think the key thing that we have as an individual franchisee or individual operator is what I call the smell test. I mean, something just doesn't smell right. There's just

something that is not good about this. And our guys get their antennas up.

Sometimes in that particular case, they'll take the initiative and either call, not always is it the Postal Service, it can be the local police, state and local authorities. We get involved in a lot of the drug scams. People use us as drops for drugs. That happens. And that's outside of the Postal perspective, but that's part of the world.

So, the key thing is to just be aware of what's going on. And we do some things at MBA both at the corporate level when we're training our franchisees and at the local level with ongoing work with the Postal Service. As a local franchisee in Maryland and DC, I meet my franchisees periodically, and I can tell you over the 15 years or so that I've been the area franchisee, we've had the Postal Service in, for example, half a dozen times over that period of time to talk with us about how they operate and how we can be helpful to them, and that sort of thing.

Now, this is all a very unofficial sort of thing. There's nothing that requires us to do that. We've just always done it because we thought it made sense to do it. We want to be a good citizen. And we are good citizens. We've got some good reps. At the

corporate level, we do so, as a part of training new franchisees, but when we train new franchisees, we do spend some time during our block doing lots of things, and the CMRA part of it is just one part of it. But we spend some time talking about fraud and scandal and how we can be used and how the franchisee should be aware of what's going on, both legally and also in terms of just trying to do the right thing.

MS. FEUER: Thanks, Alan. I'm going to have some more specific questions, but let me turn now to Andy Lynn, and since Robin opened up the issue of opening up courier packages that contain money, I'm wondering what you are seeing at FedEx in terms of frauds, particularly consumer frauds and what you do in the first instance to address that.

MR. LYNN: Stacy, thanks a lot for inviting FedEx to be part of your group here today, and I was just looking at the list of folks here on this panel, and the truth is, you know, FedEx works closely with really all of these organizations on a daily basis. Not quite as much of the Australian competition authorities yet, but we'll be talking to you soon there.

But Robin and I were actually having a short conversation before the panel, and I will tell you that between the Customs Service and the Postal Inspector,

since we're carrying a lot of mail on our air network, they can give you a very accurate idea of the sorts of things that are moving through our system. You know, there are all sorts of wrong types of shipments that can move through the system, be it cash or contraband, things of that nature.

I think Robin would tell you that the policy of FedEx really from the beginning has been, number one, we want to have, you know, a very close, cooperative working relationship with law enforcement authorities. We have a fairly large security organization, and a very important part of their job is to liaise with the Postal inspectors and the Customs and the FBI, and all these other agencies that Alan was mentioning.

Do we have -- you know, again, between the smell test, just in the express business, we have about three million packages a day. It's hard to apply the smell test to every single one of those, but the truth is there is usually a FedEx courier or employee having some interaction with the package. You know, are there profiles and things that we look for that help us kind of have a suspicion about whether something looks right or not? Yes. Does the fact that we have a very data-intensive, on the international express part of the business, we gather a lot of information that's required

for our purposes for tracking, billing, and also for Customs clearance.

So, we have a data-rich environment that, again, we are able to work with law enforcement to use when they say that they've got reasonable suspicion.

One of the things, Stacy, you and I talked about leading up to this panel is that line that we really try not to cross, which is we are about providing service to our customers, we're about protecting the brand name, the customer experience with FedEx. And let me just disclaim any interest in our having or obtaining revenue with working with fraudulent shippers. Let me tell you, that's a bad business model for you. We have salespeople that are focused on automotive industry, health care, pharmaceuticals, we don't have a fraud sales unit. We're not after those shipments.

Number one, they're not always the best to pay, but number two, even if they do, at the end of that transaction, you know, the bad guys are gone, the only number they know is 1-800-GOFedEx and that can really eat into your margins there.

But I'm sorry, my point was we want to work as closely as we can with law enforcement and we do and we will, but we mustn't let the FedExes of the world cross over that line into actually becoming de facto law

enforcement agencies on their own. We have obviously obligations to protect the integrity and the privacy of data and people shipping legitimate shipments from point to point need to not have an unrealistic fear that all people who don't need to know their business are going to know it.

MS. FEUER: Thanks. Before we turn to talk about maybe some of the specifics of cooperation short of co-oping private business into our line of work, I just want to ask Lee about her experience in Australia, and I know it's slightly different there because your relationship with the Postal authorities is different, but what do you see as the use of courier services and CMRAs to the extent they exist in Australia?

MS. HOLLIS: Thank you, Stacy. I would just like to say, by way of introduction, that as far as cross-border fraud is concerned, apart from the net, mail-based fraud is the next biggest issue for us. What we have found in practice is that there is a great deal of cooperation from commercial enterprise as well as our Australian Postal sources in helping to detect and put an end to cross-border fraud, particularly international fraud.

There are legal impediments which affect how we go about doing things, but I think generally, as has

been mentioned by members of the panel, we proceed from the basis that no reputable company would want to be associated with fraudulent conduct, and from that basis, it's very easy for us to go ahead with commercial enterprise to put a stop to fraud where that is possible.

We do have issues in the international arena with extended reshipping of checks and cash which means that's quite a long investigative trail from time to time going around the globe. I think we've had traders who might ostensibly be located on the Gold Coast in Queensland, for example, in Australia, which is a huge post office box center, and associated probably with criminal activity, but in fact, the originator of the scam may be in Canada or the U.S. The mail may be picked up from post office boxes in Australia by someone who is unfamiliar with the scam, they're merely paid to pick up and reship material, and on its way to the States or Canada it may go through ports such as Fiji and other places.

But our experience, as far as working in partnership with commercial enterprise is concerned, has been positive. I think particularly directed towards disruption, where we've become aware of frauds, we take it up with the commercial enterprises and generally

receive cooperation. And I think our next step is to work in greater partnership with commercial enterprises as well as our Australian Postal authorities to take more preventative measures to prevent cross-border fraud.

MS. FEUER: Thanks, Lee. Alan, maybe my next question will get to this, and if not, you can chime in. I wanted to just ask, you know, obviously there's a level of cooperation that's already ongoing, both with the criminal agencies and civil agencies like the FTC, but I wanted to ask if some of this could be done on a more systemic basis, and I guess there are three areas, and I've talked a little bit with Alan and Andy about them.

One is in the information sharing area. Is there some more systemic way that we can get together to share information, and the one issue I want to raise is an idea that Robin and I were kicking around, and that's of given an organization like FedEx, a corporation that uses a lot of automated systems, if we, law enforcement, were to come to you with a list of bad addresses, for example, Montreal, is there some way of flagging that in your computer so that your agents are aware that there might be something fishy about 400 packages going to a certain address?

Let me throw out two other things and then maybe we can comment on them all. Another thing that Alan was talking about was he was talking about MBE University where MBE trains its 3,000 franchisees in the U.S., as well as its global franchisees, and I guess the question there is are there more opportunities for training, and I know FedEx does a lot of training.

And then the third thing that I want to throw out here, for enhanced cooperation, and ask for your thoughts on all three, again, goes to suspension of services. What do you do when you are aware that consumer frauds and money are being run through your companies, and in terms of working with a civil enforcement agency like the FTC, what do you need from us to suspend those services? Do you need a court order, or is there something less, given by the time we go get a court order, sometimes the fraudsters will have moved on.

So, I throw out all those questions and perhaps Andy and Alan can take a stab at them.

MR. ARMSTRONG: All three?

MS. FEUER: Well, in the interest of time, I figured I would lay it all on the table and then see what people want to say.

MR. ARMSTRONG: Okay. Just two things, before

moving on to those things. First of all, although this is called a commercial mail receiving CMRA panel, so to speak, the fact of the matter is that not all the things come through the mail in terms of fraud. I mean, we take packages in as commercial mail receiving folks from not only the mail, but also from FedEx and UPS and DHL and Airborne and what have you, and it's just as likely that those guys can be used for fraud and that sort of thing as the Postal Service. I mean, it happens.

In fact, some of the biggest frauds that we've been involved in very truthfully have come where we've gotten involved in FedEx and UPS, because we accept packages, and that's not really controlled by the CMRA regulations. I mean, when we take a package in from FedEx and UPS, not part of the CMRA regulations at all, it's just receiving a package from FedEx.

The second thing before we move on, what is the cost of the individual operator, the individual CMRA in terms of this whole thing of fraud situation. Well, the biggest cost for us is our credibility. My worst nightmare as an area franchisee is to come home and be watching the 6:30 news and all of the sudden find one of my centers in downtown Washington, DC on the 6:30 news talking about it's a drop for some criminal or fraudulent scheme. That doesn't do us any good. And

that is just disastrous to us.

And it happens. And it happens across the United States. So, we're very concerned about this from a credibility perspective. That's critical to us, because it strikes to the heart of our brand and our operation. I wanted to get those two things out and I think it's critical, you know, very important, those two things.

Now, moving on to how we work with these folks, most of our relationships right now have been pretty informal. I can say this, and my colleague here from the Postal Service might not even be aware of it, but we have developed a pretty good relationship with one of his colleagues out on the west coast at the national level, and he funnels our folks at our corporate level all kinds of information about what's going on in the Postal Service, both through the scams and abuse that we then download to our franchisees through internal communications tools. And that's a very good way to do it.

I mean, we did something about once a week from our corporate headquarters talking about what's going on, newsy sorts of things in our business. And it's probably at least every -- out of every two or three of those, there's something we receive in the Postal

Service saying watch out for this, watch out for this name, watch out for this scheme that's going on. And I think that's done unofficially, Larry, I don't think there's anything official related to that. But it's an excellent tool, by the way.

MS. FEUER: So, using your internal corporate communications and having the Post Office provide that information?

MR. MAXWELL: Yeah, what you said is totally accurate. When we did the regulatory changes, one of the understandings we had with the different organizations, Charmaine as well, it would be nice if she could address this with us, we agreed that we would enhance our communications in terms of training and sharing of information. We shared email addresses from inspectors, that was done on a national level. I think it's been better served at the local level up until this time.

There's another group that's in charge of identity theft in my organization that has responsibility for that, and they're working now towards organizing something a little bit more formal from the national level. I think there's a lot of opportunity there, but I'm glad to hear that they kept it rolling from the time we had the original discussions, because

that was good.

MR. ARMSTRONG: I mean, I think the whole relationship has been pretty informal, very quasi official, so to speak. And I think it's funny in talking about that, to make it more formal would be very, very useful. Particularly at the top levels. I mean, at the lower levels this sort of back and forth is going to happen. Talking about not only from the Postal Service, but the FTC and the Secret Service and anybody else. We have a tremendous internal capability to get the word out to our guys, and I don't think it's being fully utilized by the rest of you all.

MS. FEUER: And we at the FTC would be very happy about that. I mean, one of the things we talked about a lot yesterday in our panel, since we obviously have a lot of representatives of other law enforcement agencies here, is how we can make sure that our efforts are coordinated and that, you know, Larry, we work with a lot, so he is aware of the scams that we're investigating, but I think there is an opportunity, it seems like, both with a corporation like MBE and FedEx, to partner using the corporate communications systems and that we in the government need to be feeding the data and the trends we're seeing in a perhaps more unified way.

MR. LYNN: Stacy, I think there are probably opportunities to leverage communications networks that we have. FedEx, you know, we've got an internal television network and we do ongoing training and safety, security, fraud detection, it gets right in there along with how to be safe in bad weather and not having vehicle accidents, but we would be very happy to talk to you about featuring you folks on some of our shows to say, here are some of the examples of things to be looking for, and more importantly, here's what to do.

What we would probably do is feature the law enforcement representative along with one of our security folks, which gets back to your point on the hypothetical about comparing a list of addresses and seeing what can be done to sort of see what's happening there. And what I would tell you is our informal cooperative system would already facilitate that. I would tell you to call me, call our security group, we would sit down with the law enforcement officer and evaluate the information and to the maximum extent possible we're able to cooperate to get the bad guys.

As far as suspension of service, there are some times when we need to suspend service to customers for non-fraud-related matters. So, we have ways to do that. Again, it would just involve our sitting down and

looking at what is the nature of the information and not turning off any people that were actually not bad guys. That's kind of a problem.

MS. FEUER: Right. And let me ask Larry or Robin or both of you, in terms of some of these ideas of continuing obviously the informal cooperation but doing some more systemic things, you know, either on the training end or the information sharing end, what do you see as things that would be useful for you?

MR. MAXWELL: Well, I think we heard from John Sullivan yesterday with the mail industry, and we've done a lot of things there where we have joint meetings and we share best practices. We have inspectors, some of my counterparts work with FedEx, and they've come back with glowing reports of your security network and we've learned a lot from them and we've shared information.

I think we can do a lot more from a systemic end with the commercial mail-receiving agencies, which frankly we probably let the ball drop. We could have pursued it at an even greater rate to keep that rolling, but I think our main focus was getting on the registration and identification first and also the database, but I think this next phase, there was talk of having agents at training academies for new franchise

operators. Again, we've talked about uses of the satellite networks, and I know there are some other forms we could probably use for that.

The prevention area, of course, is always the one we wanted to push and we try to share that. Any time we do stand-up talks to Postal Service, to the carriers, any time you have a false address, or in the commercial agencies, you have issues which bring it up to the supervisor and they'll talk to the operator of the commercial mail receiving agency.

So, there are a lot of opportunities there, I think we've kind of just scratched the surface a little bit, and that's why this is a good dialogue, because there's a lot more things we can do.

MR. LANDIS: I totally agree, because most of the dealings are with the security office, the banks or FedEx or the money transmitters, and we like to get the message out to the actual worker bees at the street level out there looking. They have more eyes out there that can tell us a lot more of what's going on.

And I'll just give you a real fast story that we discovered up in Montreal is that these people are very well organized. They'll do surveillances at locations for drop sites. They'll pick Stacy, they'll look at your house, they'll see when you're home and when you're

not home. If you're not there between the hours of 8:00 and 5:00 and there's nobody else there, they will use your name and your address and receive, and they will have somebody sitting out in your driveway until that package shows up. And they say, oh, I'm Stacy, I'm just getting ready to go to work, I'll take the package. And then when law enforcement comes knocking at the door, they're looking for Stacy for receiving the money.

I mean, these guys are very well organized. And when you have more eyes out there like the drivers, saying, hey, this doesn't look right. Or if we have the drop sites, where mail is being forwarded in large quantities for a foreign country, if they have a box with a return address that's different than where they're located, and sweeps. Sweepstakes, entries, and this I would like to stress this to everybody, any time a sweepstakes asks for your private home phone number, you're asking for trouble. That's what we find at 90 percent of the telemarketers, the fraudulent telemarketers are people that put their phone numbers on sweepstakes. And that's what we're finding.

MS. FEUER: Let me just ask Lee, before we move to some questions from the audience, you said that you had generally very good levels of cooperation, and I'm wondering if there was a particular example of something

systemic you do or something informal that has been done that might serve as a model for us here?

MS. HOLLIS: Well, I would refer to the general situation where we have good liaison and relations with The Directing Marketing Association in Australia, and the members include frank companies, and through that forum, it's a very good way to liaise on a regular basis, and find out how industry is viewing the world and what's going on. And particular areas or hot areas that might be developing and emerging, and also a chance for us to give something back to industry through that forum.

MS. FEUER: And that's great and that will actually lead us into our next panel this morning. I want to just leave it open for any final comments from the panelists, and also turn to the audience and if anybody has a question to raise their hand and we'll bring the wireless mic over.

Elliot, if you could identify yourself for the record.

MR. BURG: Elliot Burg from the Vermont Attorney General's Office. I had a question for Andy. I take it from what Robin has had to say is that there's still a problem with courier services picking up checks from consumers' homes. If that's the way physical checks are

making their way to Canada.

If that's true, or to the extent that it's true, does FedEx have procedures in place for its delivery people, procedures and training that would allow those people to sort of -- I want to use this in a benign way, but profile the people that they're picking up mail from to determine if they've got a potential victim. Maybe it's not an elderly person, but some situation where they can spot a victim of fraud and then try to educate the person or persuade them not to go forward with the delivery?

MR. LYNN: I think, again, you've touched on a very good example of that balancing act that we have to perform every day. I mean, the truth is, our couriers tend to know the people, and we're really talking here a residential situation, and probably the most effective deterrent that we have is just sort of the gut feel of our people. And there are certainly anecdotes where I've been involved where we get this call and someone just says, you know, this just doesn't feel right.

So, we've got 45, 50,000 couriers on the streets, and they're mainly nice people and they mainly like their customers, but if you take your question kind of just a half step further, there's really not going to be a way for FedEx or any other entity to sort of be the

guarantor of the integrity of the transaction that they're a part of.

You know, just as the mail, you know, the Postal Service, we do what we can to keep the bad guys at bay, we really want to do that, but we're not going to be able to get to the point, I don't think, of asking 20 questions about all right, Mrs. Johnson, why exactly are you sending this check to ABC company, have you thought it through. There's a point at which nobody can completely protect people from fraud, but we certainly are interested in doing it, and our people, our couriers especially, use their judgment very well in that regard.

MS. FEUER: And if I'm correct, you did tell me, though, that from time to time FedEx will open packages under your conditions of carriage.

MR. LYNN: We certainly have the ability to do that. You know, the conditions of carriage, and it has always been that way, but if in the example we're discussing, we would open a package to see who the check was made out to, I mean that doesn't exactly fit the normal profile, but again, Robin and his band of characters, of course, can open any international-bound package that they want to.

MS. FEUER: And they do.

MR. LYNN: And they certainly do, and they have

data systems to, again, officially profile the packages, and we do a lot of package opening.

MS. GRANT: Hi, Susan Grant from the National Consumers League. Two things, one for Andy and one for Larry. As an example of a proactive measure, Western Union, when you call its quick pay service, actually has a recording that says that if you're trying to send money for a sweepstakes or to make a charitable donation to firefighter or law enforcement organization, press 1, and then when you do that, you get a message saying essentially that it's a scam.

That's a good model that could be used whenever consumers are making arrangements by phone, and also if somebody is going to a house to pick up a check, perhaps there could be some written information that is given to them about scams and how they work and how to recognize the danger signs that might forewarn the consumer that maybe they're about to do something about.

So, that would be interesting to consider.

An issue for Larry, as you know, we were really unhappy with the alternative in the CMRA rules for the hatchmark number in the address, because there's no way that consumers can tell from that that they're not sending a payment to a suite in an office building, whereas PMB is much more obvious. It would have been

much easier to train consumers that when you see PMB, what that means.

We're not finding that anybody is using PMB. So, I've got a couple of questions for you. One is, are you finding that anybody is using PMB, and are you finding that the cross or pound sign number is being abused? And also, will the Post Office deliver the mail to the commercial mail receiving agency if it doesn't have either PMB or the hatchmark?

MS. FEUER: Why don't we have Larry answer and then I don't know if Andy wants to comment on Susan's question.

MR. LYNN: Go ahead.

MR. MAXWELL: Susan, with the pound sign, I haven't seen any -- I've seen both used, I've seen PMB and pound sign used. Pound sign is a little harder to distinguish, because it can get merged in with some of the other address aspects, and that is one of the things that did concern us. But the PMB I have seen used, and if they're not using either, the Post Office is under the directions to discuss the matter with the CMRA operator.

Stacy raised the issue of what alternative means we have as far as shutting down and so forth. That's an extreme measure. The Postal Service has that ability,

the district manager can shut down a CMRA franchise if they're not in compliance, if they're found not to be in compliance. And naturally nobody wants to do that, and so far we haven't had to do that. And they've been in compliance. And if there is a customer, one customer, that's out of compliance, they're not going to risk having -- and that's the whole theory behind that.

What I am doing as we speak, in fact, we're looking at a means to take the 1583-As, which is the CMRA operator, their application, that's not automated nationally. We would like to automate that nationally for our purposes just to help address the issue of this is a CMRA, this is a listing, and at least make that available so if you're mailing to it. Because right now it doesn't exist with us. It exists with the industry, separately. It's not all pulled together. And I think that most people have been asking for that and it's just never -- there was never a need before and you can imagine, with 40,000 post offices, and a lot of them aren't regulated. A lot of them don't even register that are in the legitimate side of the industry.

If you go into the Bronx or Queens or even areas of DC, you're going to find a lot of what we call mom-and-pop stores where they will take mail in for people. And, again, that's a postal delivery issue, we

shouldn't be delivering mail if we don't know who that is, but it does happen.

MR. ARMSTRONG: Stacy, can I kind of follow up on that? As it relates to the PMB, it is being used. What we do with new potential customers who rent mailboxes is explain to them how they should have their mail sent to us and what have you. But in a very practical sense, we in the CMRA industry can do our job by informing customers this is how you mail things or have things mailed to you. But when they go out and communicate and portray their address on the one hand, and how the people who send things to them use their address is impossible to regulate. I mean it's just impossible.

You know, if somebody decides to send me a card and how they put the address and how they lay it out, regardless of what the regulations have, you know, what's the practical answer to that? I don't know the practical answer to it. It's very, very difficult, though. But we can and we do do everything we can, and you say there's been no CMRA so far that you're aware of that you guys have had to put the hammer on?

MR. MAXWELL: No, there was one, there was a little discussion over some issues with one customer, but we talked about that and calmed that down.

MS. FEUER: Andy, did you have any response to that?

MR. LYNN: On your issue, number one, it would be very interesting to hear any specific anecdotes that you've got about somebody having to go out and pick up a check. I am going to tell you, I don't think we're too out of school to say that in the type of scam that you're describing where you have the boiler room operator saying, all right, I'm going to have a courier come out to your location and pick up a check, the good news about those is that those are typically, they're going to need to be billed to an account number, and it is easy once we are able to identify these as bad actors, you know, in our systems, you know, to kind of make that stop.

You know, the bad guys are agile and move around, but it would be a bit of an atypical situation for someone who doesn't have an account number with us already shipping FedEx Express, for example, to call out and have a courier come to pick up a check.

I've taken a long time to say, we're always open to other suggestions on how to improve our communications and our screening, but what I would tell you is that I think our current mechanisms are fairly good in that regard and there usually has to be one or

two victims before we catch the bad guys, but we can get them pretty quick.

MS. FEUER: Great. I think what we'll do now is move on to the next panel, so I want to thank all the panelists here for participating. It is a shame that Charmaine Fennie wasn't able to join us, although she got a lot of references, and we've heard a lot of positive things about what's going on now and perhaps ways to build on that with both the CMRA industry and with courier services like FedEx. So, thanks a lot, and we will move right along to the next panel on the role of self-regulatory organizations and industry associations.

(Applause.)

MR. STEVENSON: All right, well, why don't we move on to our next panel, which is the role of industry associations and self regulatory organizations and the role that they might play. And we have -- I think the panelists' bios are in the material, so I just propose to jump right into the discussion, and I think that the question to start with is what role is it realistic to expect that industry associations might play in partnering with law enforcement? Obviously there are roles that they have, legitimate roles in advancing the industry's other interests with law enforcement, but

what kinds of roles is it really realistic to expect that industry associations can play in partnership, and how might we see them, what kinds of examples do we have?

And I'm going to actually look for a volunteer to answer that question, if somebody wants to put a tent up and venture a thought on how they might see that question. We will have a volunteer, even if no one puts their tent up, but --

MR. WHITELAW: All right, all right.

MR. STEVENSON: Bob Whitelaw?

MR. WHITELAW: Yes, I think number one in terms of the Better Business Bureau system, there is no border, no cross-border matter, and that with our counsel in Arlington and the counsel in Canada, we share a lot of information. And on the positive point, we're not bounded by a lot of regulatory requirements.

The best way of the partnership and idea is Ken Hunter, former Chief Postal Inspector of the United States, has sort of put our mandate up, and that is when a consumer, a business, or an organization is about to spend money or donate money, we want to be there to reduce their risk.

Now, we, in terms of receiving information, have the opportunity to deal with awareness, accessibility to

just-in-time information, responsiveness, and redirection, and without too many seconds passing, we can get information out to the bureaus, the 140 throughout North America instantaneously. At the same time, move information to the media, and more importantly, to governments, whether it's the Competition Bureau in Canada, the Federal Trade Commission, the Office of Fair Trading, move that out, get it out to the business community.

Almost in an, as I say, within seconds of information, that's one of the main tools of this regulatory or nonregulatory work that we do without having the checks and balances. We can name names. We can name issues. We can name addresses. And that is helpful to consumers, businesses, organizations, and government groups.

MR. STEVENSON: Let me ask, maybe Mark Bohannon, we were talking earlier about this issue and the kind of role that the industry associations might play, and it may be also obviously that industry association may mean something slightly different from the role that the BBB can play, but, Mark, I think you had a few thoughts on that.

MR. BOHANNON: Yeah, sure. I appreciate your comment, Hugh. We are not a Better Business Bureau,

though we have tremendous respect for what the Better Business Bureau does. We are an association that has companies as members. Those companies range from some of the smallest in the technology area to some of the largest, and even, you know, along that range, they face a variety of fraudulent acts, both here in the United States and abroad.

So, that is an area particularly in what I would call and what you probably understand as the counterfeiting areas, a place where we do a great deal of work with a variety of law enforcement authorities here in the U.S., and as appropriate and others, particularly Canada, Mexico, and to some degree the United Kingdom.

We see and are asked by our members to play a variety of roles in working with law enforcement. They range from being a source of information and helping to keep government enforcement authorities up to date on new models of what we see as fraud and counterfeiting, in a world that advances as technologically quickly as our world does, it is a challenge for everyone to keep up with what is going on in the new models and approaches to fraud, and certainly we see our role as being both a formal and informal source of helping to understand what those new models are.

And we do that through white papers, which you will find on our website, we do it through informal dialogue, we go to meetings, and quite frankly responding to calls as appropriate.

The second role that we often and significantly play is being an interface between our member companies and law enforcement in situations where either there may be criminal or civil action brought against someone, and where the company either does not have the bandwidth or is not comfortable with being a direct interface as well. That often involves in our case being a hotline for tips for those who pirate or counterfeit our company products. We have a very sophisticated operation that goes back at least 15 years working in this area. We have clear issues and policies about the anonymity of that data, and at the same time, over the years, we have developed a solid reputation with law enforcement that what information you get from us is going to be very real and very serious.

And I think the third area, as appropriate, is coordinating on appropriate enforcement actions when fraud is actually found. The reality is that both in the public and private sectors, there are not all the resources to go around. In some cases, it is appropriate to bring criminal action, some cases it's

not, and so as appropriate, and within appropriate boundaries, those are areas where we interface as well.

So, Hugh, those are some of the examples. I would be glad to explain more, if you want me to go into more detail.

MR. STEVENSON: Thank you. Maybe I would ask next Jerry Cerasale how the experience with the Directing Marketing Association compares with the experience that Mark just described for the Software Information Industry Association.

MR. CERASALE: Thanks. The Directing Marketing Association has its own internal guidelines for its members and an ethics procedure dealing with and split up in two with telemarketing and then all other ethics procedures.

The goal of that kind of self-regulation is to try and get things corrected, but if we find in the course of this investigation, which is done by peers of the member companies, and we have no individual members, but 5,000 corporate members, we will then transmit the information we find to the appropriate legal authorities. If we find, in fact, there appears to be a violation of law, be it the state AG, be it the Federal Communications Commission, the Federal Trade Commission, et cetera.

One of the things that where we really work well with the Postal Inspection Service, and I think you had a member of the panel yesterday discuss it, bad addresses, identity theft kind of things where an identity theft is a crime against me, the individual, it's also a crime against me, the company, if you're going to try and purchase something and end up not paying for it.

So, there are a lot of addresses that where that happens, and that information gets out and you know that 123 Main Street of this town is generally an address to be leery of, and we work with that with the law enforcement community and spread that word around, because that can help prevent a continuation of the fraud and try and find someone.

A lot of times the cross-border fraud, unfortunately, except for the lottery issue that was raised, I mean that's illegal on its face, and members should know that, they're required to know what kind of pieces go out and how lists and so forth are being used. But many times, the fraudsters break up their activities. They may control the telemarketer located in Canada, we're dumping on our poor neighbor in the north, but located in India, located in Bangladesh, anyplace where they think that they can go into the U.S.

where there's a different English, or even a Spanish country if they want to come into Spanish-speaking Americans and so forth, they can control them.

But they get a list from somewhere and the list provider takes a look at the script and the script looks fine, because the fraud happens with, I send the money in and I don't receive what I paid for. And they could use a printer, the printer, the printing looks fine, it could be a very legitimate offer, if, in fact, they do that, and so you don't know.

And so that's part of the problem that we face from the point of view of this type of fraud, which we all want to try and get ahold of, even information, if it's not obvious on the face of the piece of the campaign that you're dealing with, you're not going to catch it. It's a requirement of our members to take a look at what your piece is, what the piece of this campaign is. If you're sending a list, what's the providing list being used for? Well, it's being used to sell such and such. And you send the money in and you don't get it back.

Well, the list owner is not the fulfillment agency, so they're not aware of it. They can even see the list, so that you're going to call Jerry Cerasale's home, even though I'm not on the -- normally on a list,

I'm just going to see what's being said and I can listen to the script, say, no, I'm not interested, because I'm not going to spend $1,000 or the $100 or whatever it is, but the script sounds legitimate. And that's part of the problem that we face.

So, I think that if we find information we have to get it to you. And we have to work, I think, within our DMAs throughout the country. You heard about Australia working with their authorities, and Alistair is here, as direct marketing associations have to work together to try to spread information. I think that's the biggest key. The problem that we all face, though, the one fear, and I'll just say it, is spreading the information, does it make you automatically knowledgeable and liable for it, and therefore our members will then not become volunteer members of the association any longer. So, we have to worry about that kind of thing.

MR. STEVENSON: Okay. And that's an interesting point. And maybe, as I understand it, just by way of background, a lot of your members are indeed suppliers or the service bureaus who are involved who might be the entities who were seeing these various pieces that you describe, and so one of the challenges is the role that they're playing, and you're talking about their

incentives to be a member of your organization.

MR. CERASALE: Right. And, I mean, it is -- they don't want to -- as they said in an earlier panel, you know, having a fraud model is not a good business model generally for a legitimate business player, but how do they know? Because in essence, there's the fraudsters are putting a fraud upon the suppliers, some of the suppliers, anyway, using their facilities to perpetuate a fraud, but keeping that knowledge away from the supplier. And we have a lot of suppliers.

MR. STEVENSON: And, Jerry, I know the DMA has, I think you referred to this briefly, a code of conduct that applies to the various members, and I think there are provisions on the supplier service bureaus. Is one possibility, of course, there is the fear that you mentioned, but is one possibility thinking about adjusting that code in some way so that people are -- have some role in trying to see the larger picture?

MR. CERASALE: I think that we -- I think that's worth a good series of discussions as we come out of this and what the authorities do, what the Federal Trade Commission wants to do, and try and get our -- not just us, but the international brotherhood, and Alistair may talk to that, of the DMAs, to take a look at what type of thing we can do and how we can make an adjustment. I

think that that makes some sense, because, you know, fraud hurts the entire business, so it hurts our legitimate members to have cross-border fraud. So, you want to try and end that.

But working it that way, but not becoming the police force on our own sense, because we can't, that's not our role, and but to work in that way, I think, yes, we can look at that, we can try and see what we can get together, what law enforcement needs, what we're able to provide and so forth.

MR. STEVENSON: Can you say just a little bit more about the fear issue, or the liability issue, maybe just to spell it out, put that on the table. What, sort of, are the bad things that could happen there?

MR. CERASALE: Well, I think the bad thing that can happen is that you suddenly don't have people being members of the DMA if, in fact, we work with law enforcement. And we get information that we distribute to our members. And then that becomes, in legal terms, actual knowledge, and therefore then the supplier would then be held because the DMA put this information out, to then become a knowing participant in the fraud.

That's the kind of thing that we have to be careful of, not to cross that line, because then that becomes a disincentive for even legitimate companies who

could be caught up with a small piece of someone purchasing something from someone to drop out of the membership and then that would lose, it would hurt DMA and it would hurt me, since it would be my salary, in part, but it would also hurt the cooperation side, if you have outliers.

Now, some of the suppliers in these frauds are clearly legitimate companies that are probably members of many organizations and want to do well. Others probably may not be, but at least you want to keep the good guys that are there trying to work in that direction and not give them a disincentive not to cooperate, in that sense.

MR. STEVENSON: Okay. Maybe we'll turn now to Alistair Tempest, and your role that Jerry described as the international brotherhood, or at least the international aspects of direct marketing associations, and how do some of these concerns that Jerry mentioned play out internationally? I guess one thing I'll mention to put this in context, and Jerry referred to this briefly, but this issue which is the outsourcing of various capacities.

There was a cover story on a recent business magazine about call centers being outsourced, and they cited to the Philippines, to India, to Costa Rica, South

Africa, Mauritius. I mean, this is a phenomenon in terms of how the legitimate industry is going, I take it that's fair to say, and so that raises the question of what implications does that have for the illegitimate part of the industry, and is there a role that the related organizations can play in addressing those problems?

MR. TEMPEST: Thank you very much. Well, firstly, I would just like to comment very quickly on a point. You said the illegitimate part of the industry, of course it's not part of the industry. We would get rid of it if we could.

Turning to what brother Jerry said, from the brotherhood, we're faced -- perhaps I should say a little bit quickly about Europe, because it is somewhat more complex. In Europe, we're faced with a patchwork of regulations, self-regulation, which makes things very difficult. In some countries, self-regulation is very well developed, particularly, for example, in the country that I originally came from, the UK. In some countries, for example Germany, the law is used.

There were some lovely statistics some years ago where the advertising standards authority of the UK were looking at something like 2,000 cases, and about something like 60 were going to the courts eventually.

Whereas in Germany, exactly the opposite, there were about 2,000 court cases, and only about 60 cases going to the self-regulatory body and there was that overlap. So, you can see from that that there is a very big difficulty in giving an easy answer to your questions in Europe.

What we clearly want, and I want to stress very much what Jerry said, the issue of confidence in direct marketing is very much at stake here. If there is more fraud, then the more fraud there is. And I would include within fraud harmful spamming. Then direct marketing and the acceptance of direct marketing starts to be very, very seriously undermined. I think that we can see some rather nasty experiences in Central and Eastern Europe where the people were much more naive because they had never been approached before, and then of course you've got the fraudsters going in doing all sorts of perpetrating or all sorts of crimes against humanity, imparting from the unfortunate consumers large amounts of money, at least relatively large amounts of money.

Now, in some countries, for example in Poland and the Czech Republic, there is a resistance building up to buying at a distance, within their own country, farther outside. So, one has this serious problem

starting in some of the new democracies. As I think Donald Rumsfeld recently called it, the new Europe, the new energetic Europe, not the old tired Europe.

So, in terms of looking at the way in which self-regulation is operated in Europe, we at FEDMA have a number of codes, we have a code on e-commerce, we have a code which is being negotiated with the regulators on data protection or data privacy. We have codes on list brokers, we have codes on telecommunications -- teleservices, and we support the preference services or Robinson lists at the national level.

We can only do that through the national level, and with the support, of course, of the national level, and of the direct marketing associations at the national level. Or if it isn't a direct marketing association, sometimes it's a self-regulatory body. What we're also doing, as Charlie Underhill mentioned yesterday, is working with the Global Trust Alliance, very much, to try and build that up on the global level.

What we, I think, what I would like to say is that I feel that there is a problem, a problem not only in Europe, but also outside Europe as well, where different authorities and different organizations and different self-regulatory bodies are looking at different means of communication, and that creates

artificial, particularly nowadays, artificial differences in the way in which certain forms of communication are dealt with. And that is a problem. It creates a problem, because, for example, in e-commerce, you may have one type of rules, created by one authority, or one self-regulatory body, and in mail we have something else. So, we have this unbalance.

MR. STEVENSON: Since you're tired, I don't want to overtax you, but just to follow up with one question. Jerry mentioned the DMA codes which do have some provisions on suppliers and service bureaus, in other words I'm thinking of the ones that apply to just the third parties if you will, as opposed to the marketers themselves. Do you all or do your members have provisions like that? Is there a common thread in terms of what those provisions provide for? Could there be? Would there be some value in doing that, and would your membership have the same fear that Jerry mentioned?

MR. TEMPEST: Hugh, thank you very much, indeed, because this is a particular issue at the moment. Firstly, again, I have to stress the difference from country to country; however, having said that, some of our members, for example, the one in Belgium, not only has the right to fine its members, and indeed it's done that if it can get at them, for providing services to

known fraudsters, but also there is a case which just came up this week in the UK, the vice chairman or one of the vice chairmen of The Directing Marketing Association UK has been nabbed, I don't know if that's the right wording in American, but caught because consistently her agency has been providing services to a couple of known fraudsters.

Particularly time share, time share is a big thing in Europe, I don't know if it's so much here, but this is one of the fashions now, so-called Spanish -- the Spanish fraud. And she has been -- she's been put under investigation and is very likely not only to be thrown out of her vice chairmanship, but even to have her agency banned from the DMA UK. So, I think a very good example.

Now, liability, we're not quite so litigious in some respects in Europe. So, we don't have quite that problem, except that I personally have that problem being in Belgium, we send out alerts for our members when we have well-known fraudsters wandering around. Officially, I could be caught under Belgian law and sued, because under Belgian law, I am not allowed to say that. Under UK law, I could say that. So, it's a problem.

MR. STEVENSON: Well, I would like to turn now

to our two law enforcements on the panel to get their reactions to some of the comments, and I guess particularly maybe the issue that the tension have raised on possible liability and what effect that might have, and maybe start with you, John Mercer, from the Competition Bureau in Canada.

MR. MERCER: Thanks, Hugh, and I certainly welcome the opportunity to be here in the last two days. I found this an excellent dialogue.

On liability, of course, there is a potential antitrust liability in terms of cooperation, and that's a cautionary note, but it's the issue whereby within trade associations, within self-regulatory groups, people cross the line and go from that which relates to, for example, fraud, and start dealing with competitive variables that are important to a viable competitive market, so it's just getting into discussions of price, market sharing and so forth, and of course I know that no one in this room would be tempted to do that. That crosses the line, and that would cause concern, and that certainly creates a liability.

I guess picking up on some of the other issues that have been raised, I think it's very important to know who your members are. I think that's another kind of issue that has arisen, certainly within the Canadian

context, and some cross-border contexts. We have certainly been dealing with some respectable -- apparently respectable marketers.

I remember a couple of years ago I went to a concert and I opened the program and much to my shock, the sponsors of the concert turned out to be somebody who we were investigating and who was, in fact, subsequently, he and his colleagues, were arrested, and I guess faced some considerable time, and I guess time, first, before the courts. So, that kind of thing becomes very important as well.

Another thing is, know who you are supplying, if you're a trade association, if your members are a trade association. This is a good area in which there needs to be dialogue. In Canada, we have under our telemarketing law an injunctive proceeding against third party suppliers, such as telephone companies and so forth, who are supplying product to people who have been across the line once in deceptive telemarketing.

So, that becomes an important element on the liability side.

I guess the overall view, however, on the role of the private sector is, first of all, we can't do it alone. Law enforcement can't do it alone. We require cooperation, we need cooperation, we need that informal

network. But the other thing is, public education is an important vehicle here, because we're never going to get all these people, and I would hope that the private sector would get involved in such organizations as NWCCC, National White Collar Crimes Center, and the National White Collar Crimes Center Canada, which has been set up in order to have that dialogue. It's a good place for dialogue on trends in law enforcement, but it's also a good place for assistance and perhaps funding public education.

We have in Canada something called The Mass Marketing Fraud Forum, in which we have involved a dialogue with our partners in the United States, the Federal Trade Commission, the U.S. Postal and the U.S. Department of Justice, and what we need there, we have a steering group which has private sector members, but we also have a primary group that has private sector members, and ultimately we will be looking to them as well for funding out of their in kind, or through dissemination. That also becomes important.

It's a way to protect both your members against fraud and also to assist in sensitizing the public to these kinds of fraud arches that are around. So, that would be certainly a strong recommendation. And I guess finally, one could talk about the codes of behavior and

enforcing those within the context of self-regulatory groups or within certain trade association arrangements.

Thanks.

MR. STEVENSON: Thanks, Don. And you were mentioning in making the defendants face the music, reminds me I should mention to people that there is going to be a press conference today, in case you're not aware, here at I think it's 1:00, is that right, on a joint Canada/U.S./Mexican enforcement initiative. So, very timely, given the subject of our workshop.

Let me turn now to Dan Nathan who is with the Commodity Futures Trading Commission in the United States, but who is in a more specialized area but has had some experience with dealing with the self-regulation in that area, and Dan, maybe you can react to some of the comments and particularly some of the concerns that are raised here and how they play out in your area.

MR. NATHAN: Yeah, thanks. Actually the comments here are helping me focus my remarks. I came to the FTC with the idea of speaking about the National Futures Association, which is the self-regulatory organization that assists us in regulating the futures and commodities industry. I'm with the Division of Enforcement, and as was just said, the government has

limited resources and we rely heavily on the NFA and other SROs to help us do the work that we have to do.

When you talk about the liability issue, our SROs may have an advantage over others, in that they are protected and created under color of law. The NFA is a registered futures association established under our act and it is given certain powers and it has the ability to take on more powers as they are delegated to them. Over the years, the commission has made a habit, every so often, of delegating more and more powers to the NFA to help us in what we do.

The implication of your question, Hugh, as to what role is it reasonable to expect a professional organization to play, I guess is that there are limitations, possible limits on the aggressiveness or effectiveness of professional organizations as to who they represent, who pays their freight. They're professional organizations and they have members, in addition to maybe limits on their authority, and there are also liability issues. Based on what I'm hearing here, and based on what I have seen in my own experience, I don't see a problem with the first prong.

The NFA specifically views it in their interest as being in their interest to make sure that the futures industry has kept clean, that those members who are

above board and are not, you know, scamsters, are thriving in an industry that is not dragged down by the bottom dwellers. So, they're doing everything they can to keep things clean there.

On top of that, what I think I've noticed, and they do an excellent job, and although I'm not typically a believer in government competing with the private sector in certain roles, for example school vouchers, in this case, I see it as functioning very well. We have a very aggressive enforcement division, and they have a surveillance and enforcement group, which is similarly very aggressive and we are always trying new things.

We both have a fair amount of flexibility, although I have to say, being nongovernmental, being essentially a private sector organization, the NFA has a great deal of flexibility in the ways that it can investigate and the types of evidence that they can gather and the uses to which they can put it. And there's a sort of spur to friendly competition. We egg each other on. And at the same time, we work and coordinate very closely together.

The second area in which the NFA and other professional organizations or SROs might be limited is simply limits on their authority. We as a governmental entity have the ability to subpoena, we have extensive

information-sharing agreements with other nations, and we can obtain a lot of information that they cannot obtain. And that is where we come in. We carry a badge. We have the ability to gather that information, so when the NFA and we coordinate on what we're doing, which we frequently do, we speak every month, we meet up at a number of association meetings, we talk about what we're doing and we divy up our work.

All of the day-to-day, mainstream kind of bread-and-butter customer fraud type cases, single brokers ripping off single customers, the NFA generally handles. They have a full docket of those cases, they've become quite expert at doing them, and they generally end up in finance that are sufficient to -- and penalties sufficient to put people out of the industry for some time and hopefully reform them or keep them out forever.

The larger matters, the more systemic matters, the matters that cut across both the regulated and unregulated industry are the ones that we take, and we take them usually with some help from the NFA, in the audit functions that they execute, in the document review functions that they carry out, and we take those and then finally we come to one reason why we're here today, cross-border.

NFA has the informal means and the contacts to obtain information from other nationalities, but nothing formal, and nothing enforceable. We, as I said, have many formal MOUs, many informal information sharing agreements, we're an active member of IOSR, which is the International Organization of Securities Regulators. When the NFA comes up against that border, we have been able to obtain information, and here's the best part, the treaties that we enter into with other nations for information sharing allows us to provide the information to our SROs for the performance of their routine surveillance and enforcement duties.

So, it comes full circle. We have powers that they don't have, we can use our powers to assist them, and at the same time, they have the ability to fill in all the gaps to do the more day-to-day stuff, the less systemic stuff, and together I think it's fair to say we blanket the industry and hopefully do an effective job.

MR. STEVENSON: Thank you, Dan. Before we go to break, I would like to offer a chance if people have any questions for our group of panelists here.

(No response.)

MR. CERASALE: They need a break badly, I think.

MR. STEVENSON: Well, we're going to give the last word to Bob Whitelaw, then, before we go to break.

MR. WHITELAW: Hugh, if it's possible to put the map up for one minute, yesterday you saw a map of North America, and I just would like to point out in our findings, these are advanced loans targeted, we push-pinned, it's on here. We've found one interesting variable that we reported immediately to the FTC, in New Orleans, and in Phoenix, very few advanced loan inquiry victims, negligible compared to the rest of North America, and the reasons are this, and we're looking at this group as to action plans and how to get right back to the initial potential victim and stop it there.

The New Orleans paper has an advertisement every day in "Money to loan, advanced fee loans or credit offers, companies that do business and ask you for a fee up front, that's illegal." This message brought to you by the newspapers named and the FTC.

And in Phoenix, "Notice: Under the advanced loan section, advanced loan fee brokers need to register with the Arizona State Licensing Commission." Those appear in the papers daily.

Thank you, Hugh, just for the extra moment to butt in, because I'm not talking about BBB today, we're talking about ways and means of awareness, and those two little advertisements have probably saved a great deal of heartache, heartbreak and identification theft from

individuals in the Phoenix and New Orleans area. And the map shows why. Thank you.

MR. STEVENSON: Thank you, Bob, for sharing that. Oh, we do have a question in the back here.

MR. TORRES: Frank Torres with Microsoft. I agree that education can play a great role in helping to avoid some of the fraud, and certainly the self-regulatory programs to the extent that you can have something enforceable to get to the members, to get them to comply, what about the outliers? What about the people that aren't or the industry groups that aren't part of a self-regulatory program?

So, I guess my question is, how can we all who are participating in the self-regulatory efforts help the FTC kind of help enforce the outliers that are outside of those bounds. Does that require additional registration, more cooperation? I guess it's almost a question for you, Hugh, is how can we be more helpful, how can the DMA and others who participate in these industry programs be more helpful to the FTC and other enforcement?

MR. STEVENSON: I would be glad to venture a comment.

MR. CERASALE: I'll take a stab at it. Frank, I think one of the things that we have to do is whatever

group we are in self-regulation, we have a mechanism to gather information. I mean, we have a complaint process at DMA, others can have some other means. We don't always get complaints on members, and I'm sure that anyone else has that kind of a process gets some outliers in a sense, and you have to try and deal with them within -- we have a fairly formal process, so you have kind of a due process, although we're not a government entity situation, to try and get it corrected.

If not, you then hand it over to the Federal Trade Commission, or if you see that it's fraud on its face, you hand it over there, or if they're in Arizona and the Arizona AG or whatever. So, I think we already do some of that. I think that one of the keys for us is the education of people. If you have been defrauded, you think somebody has, here's where you complain. And they will, BBB gets information, or maybe we need something, there's a whole list of places to complain and try and get that going so we get more information and work it through our own current processes.

MR. STEVENSON: Alistair?

MR. TEMPEST: Yes, thank you very much. I think it is a very important issue, I think that there must be much more cooperation between not only within countries,

but also between countries. And in particular, what we're seeing in Europe, you've seen here, or vice versa. We're going to experience things that you will find here in later times.

So, therefore, the sort of cooperation between the FTC and, for example, the European union, are extremely important. The European union has just done a new or is just starting a new initiative, for example, a system to -- what's it called now? It's called -- I have it written down here but I can't find it. Oh, yes, creation of a European Network and Information Security Agency.

Now, that's a very good idea, but obviously that should work very closely with the FTC and with the Canadian authorities, with the Australian authorities, et cetera. We will still end up with some people sitting on a Caribbean island somewhere, but then that's a different question.

MR. STEVENSON: We'll take perhaps one more question from Susan Grant.

MS. GRANT: Susan Grant, National Consumers League. One reason why the National Futures Association works so well is that membership is compulsory for futures traders and it has that sort of quasi governmental character. I know Canada has been or was

planning to experiment with forms of co-regulation for certain kinds of industries where membership and self-regulatory organizations would be compulsory and they would have certain powers to enforce against their members, and I would like an update on that, whether or not that's actually taken place or whether it's worked and just a reaction about that model for this kind of industry.

MR. STEVENSON: Bob or Don, could you comment?

MR. WHITELAW: I can't comment on that. Don?

MR. MERCER: Well, certainly cooperation across the border is very important. What we find in Canada on the consumer's side, for example, is that we have a number of organizations, a bit of fracturing in the consumer organizations in Canada, which makes that a little more difficult. They're more articulate and correct than they are in the rest of Canada, but I don't think I've really answered your question. Can you elaborate?

MS. GRANT: I'm sorry.

MR. MERCER: There is a mic coming behind you.

MR. STEVENSON: We can pursue, but I think the question was was there some move in Canada towards a more compulsory membership in organizations, and I think Alistair mentioned that at least in certain European

countries that is the case, obviously in the United States that is not the case, and so --

MR. MERCER: I think in Canada we're not moving towards compulsory membership in organizations; however, when we get into the issue of voluntary codes is clearly the idea that perhaps those organizations getting into those codes might want to try and enlarge the number of people within their tents, so to speak, to be effective, and certainly that has been the case where that has happened. On the other hand, enlarging membership is not always a good idea, if you don't know who your members are, and that has been proved in a couple of cases.

So, I don't know whether -- I guess in some cases, the compulsory aspect of membership has worked, it's not clear to me that it is always of net benefit to have compulsory membership in organizations. It raises other questions about freedom of association, and what the objectives of those members are in -- within those particular organizations. I don't think it's a model that we would embrace.

MR. STEVENSON: Thank you, Don. And I would like to thank our panelists here. I think we do hear some consensus on both that there is some role for various kinds of industry associations, but also there

are some limits to those roles, and we've heard some variations on how those industry associations or self-regulatory organizations are set up and also some of the possibilities for working across borders and using them across borders.

So, I would like to end by thanking our panel very much for participating and we will go now to a short break. Thanks a lot.

(Applause.)

(Whereupon, there was a brief recess in the proceedings.)

MR. STEVENSON: All right, I think we're ready to start. For those of you tired of the old economy, let's move on to the new economy. And we have to introduce our Internet panelists. One of our commissioners here at the Federal Trade Commission, Commissioner Swindle, who has been involved in a number of the international issues that we have encountered and including playing a leading role in the development of security guidelines at the OECD, and so Commissioner Swindle has offered to make a few comments to kick off our Internet discussions.

COMMISSIONER SWINDLE: From stage right. Thank you, Hugh.

This is like a group of Baptists, I see

everybody is on the outside talking politics or something, but I would like to express a good morning to you and thank you for coming on a cold wintery day, although it's getting to be pretty nice out here now.

I was in Hawaii over the weekend and could not get home Monday afternoon because we couldn't land. I got here on Tuesday afternoon, and got to my home, I wasn't sure I would be able to do that. I got to my home and had to literally dig into the house. The first thing I did was plod through about three feet of snow, go in and get a snow shovel, and come back out and dig my way through to the house. There was a four-foot drift up against the door. It was quite a shock.

It's a pleasure to introduce these two panels which are going to focus on the role that the private sector entities involved in the operation of the Internet can play in helping us combat fraud.

Let me set the stage here by noting that global electronic commerce benefits businesses and consumers alike in many ways. It dramatically reduces the time and cost between buyers and sellers, around the world, it increases choice and convenience for consumers, and at the same time it also creates new opportunities for fraud. In fighter pilot lingo, this is a truly target-rich environment.

The issue of Internet fraud is of particular concern to us here at the FTC. We have used our civil enforcement authority to bring over 250 law enforcement actions and against some 785-plus defendants engaged in Internet fraud. But the scam artists know that the FTC and our foreign counterparts still face significant obstacles when these scams cross borders.

Internet scammers can register their domain names with foreign domain registrars, they can use foreign ISPs to set up websites and send spam email, they can switch service providers and domain names to help stay a step ahead of any law enforcement activity.

As you heard yesterday and today, we and our counterparts have been hard at work trying to implement the very strategies to fight the problem of cross-border fraud, including cross-border Internet fraud, but governments alone cannot do this. Public/private partnerships are essential in combatting fraud in general and certainly cross-border fraud related to the Internet from the very systems they're associated with.

The recent OECD revision of the guidelines of the security of information systems and networks is a good example of public and private partnership working well. We had representatives from industry and the civil society working with and advising the U.S.

delegation, which I had the honor of leading. We also had representatives of both groups participating in the OECD discussions. The private sector had considerable influence on this effort and the final results. Because of the broad public/private sector participation, I believe the revised OECD security guidelines published this past year are far more useful and relevant than they would have been had government managed this project alone.

I have also called upon governments and consumer groups and industry to work together to create a culture of security, based on awareness, accountability for our conduct and taking actions that we as individuals, families, firms, workers, students, teachers and organizations can take to foster safe computing. The same principles apply when it comes to fraud.

We are all involved in this, we are all in this together, industry, government, civil society and the public in general. We're all participants and we must work together to minimize Internet fraud. This will help us achieve our shared goal of a safe, competitive, and a robust global electronic marketplace.

With that brief introduction, let me get to the Internet panels. The next panel will explore the circumstances under which ISPs and web hosting companies

can share information with law enforcement agencies and help put a stop to fraudulent websites. After lunch, there will be a panel on cooperation between law enforcement agencies and domain registration authorities. A key issue for this panel is the whois database, the starting point for most Internet fraud investigations.

How do we ensure that law enforcement agencies have access to this important information? How can we best work together to make sure that the information therein is accurate? I encourage the panelists to focus on the positives. It's important for us to discuss impediments to public/private sector cooperation in this area, but I would also urge panelists to try to address innovative approaches to creating partnerships to further our shared goal of fighting cross-border Internet fraud.

I have never been one to readily accept why we can't do something. I believe that most problems can be solved, it's just a matter of focusing on it and getting it done.

Finally, I would like to thank all of our panelists. The upcoming Internet panels have particularly impressive international representation, including participants from Canada, the United Kingdom,

Germany, the OECD and Australia. The civil society in the presence of EPIC is on board, and it should make for a very beneficial and lively discussion, and I thank you all very much. And I'll be watching on TV from the floor upstairs.

MR. STEVENSON: Thank you very much, Commissioner. I appreciate the remarks, and to pick up on something that the Commissioner referred to and that I know he has pressed in the security context is the culture of security. In the sense here, we are trying to press forward with a culture of consumer confidence and to do that by developing adequate enforcement and partnerships.

We'll turn now to the ISP and web host panel. This squarely poses some of the challenges that we face in a lot of our Internet cases, and we've brought a lot of Internet-related cases, a lot of these have a foreign component, and one of the issues is, so, how do we get the information we need to go from stop to go and actually bring the case?

I thought what we would do here to start is have Eric Wenger, who is from our Division of Marketing Practices and has been involved in a number of the important Internet cases that we've brought, describe from the enforcer's perspective where we start. Say you

know that there is a website or an email that's the problem, well, where do you go from there? How do you get the information, what issues do you encounter in dealing with the Internet infrastructure and how do you address that? So, we'll start by having Eric make a couple of comments about that and then turn to our other panelists.

MR. WENGER: Thank you. Because of the privatization of the Internet, it is vital for us to get information from the private sector when we're conducting law enforcement investigations. So, where we start typically is with the website. Let's say, for example, that it has some suspicious elements to us, and we want to figure out who may be responsible for it, so we can evaluate whether or not we want to take some sort of law enforcement action.

So, as Commissioner Swindle noted, the first place we start, typically, is with the whois database. And so, for example, I've put up on the top left screen there, a screen shot from one of our cases that involved a fake Yahoo page that was supposed to be a sweepstakes, and it lured people into downloading software that caused them to incur very high telephone charges, $2.99 a minute over a 900 number line. Which they were told was necessary in order to claim a prize that didn't

actually exist.

In any case, in this example, the first thing we would do is to look up in the whois database to see who is the registered owner of the website, and the subject of the information that's in the whois database, which I'm sure you all know is freely available, and how accurate that information is, will be the subject of a later panel, but suffice it to say, if that information is accurate, it's very helpful to us, because it allows us to identify who it is that is the registered owner of the domain name for the website.

And if we had the ability to search the database, for common elements, like addresses or telephone numbers, or email addresses, we would be more likely to be able to locate common websites that are registered to the same person. So, that's also an issue for us is once we've identified who might be the registered owner of a domain name, if we can identify the scope of the problem, what other websites they may have, it would help us to evaluate the strength of our case.

And then there are typically two pieces of information that we would look for from other companies that we know through the whois database. We typically would be able to identify the registrar for the domain

name, and also a web hosting company. This particular example, there was not a separate domain name that was registered, but assuming that there was, we would turn to the registrar and ask them if they had information about the source of payment for the domain name, and also if they had captured any electronic information at the time of the set-up for the domain name, such as an IP address.

And the same would go for the web hosting company, we would turn to them and ask them if they had payment information that would give us a money trail and also if they had collected some sort of Internet protocol address that would hopefully get us back to the person or persons or entity that set up the webpage.

Of course, there is in these cases, we use subpoenas, because the registrars would require them and the web hosting companies or Internet service companies were required to use them under the Electronic Indications Privacy Act. But that's the basic structure of what we're looking for. And that's probably it.

MR. STEVENSON: Well, suppose the information in the whois database may be inaccurate, you're relying on the information from the web host in this case to track who is behind the website. What happens if you can't get that information? If you can't trace back through

that line?

MR. WENGER: We do try to trace the sources of payment as a mechanism. We try to deal with consumer complaints to figure out if they have information about who they may have paid, but the electronic information is vital to us, and if we can't get it because the information was never logged, or we can't get it because the information was logged but was deleted before we were able to get to it, or if we can't get to it because the company that has the information will not abide by our request for confidentiality, then that avenue of investigation is dried up for us, and it becomes a major problem.

MR. STEVENSON: Okay, so speed is important in response, and confidentiality is important, I take it, maybe you could just say a few more words about that.

MR. WENGER: The investigations that are conducted by the Federal Trade Commission are required to be nonpublic, and so if I go to ask a web hosting company or an Internet service provider for information about a subscriber pursuant to a subpoena, and they say to me, we'll give you this information, but we're going to notify the subscriber, that might be an impediment that would make it impossible for us to get the information from that source, because it would disclose

the existence of the investigation, and that's something that we're not permitted to do.

And the timing issue is also very important. As you mentioned, if I want to trace from a website to a user, there are a number of different layers that I have to go through.

If I go to the web hosting company and they give me an IP address that leads back to an Internet service provider, then I need to tie that back to a user account, and hopefully to the actual user's computer, and that may require me to go first to the web hosting company, then to the Internet service provider and then possibly to the telephone company, and if each of those steps takes too long, then the data, even if it was recorded, might be gone. Or if somebody won't abide by our confidentiality request, then I might not be able to get to the level of information I need in order to trace the activity back to the person who is perpetrating it.

MR. STEVENSON: Thanks, Eric.

Let me now turn to a couple of our panelists. Let me make sure they're here. Sarah Deutsch from Verizon, sorry, and ask you just to maybe respond first to the basic scenario that Eric has laid out here in terms of responding to a domestic enforcer, say the FTC, and then what additional complications there might be if

it's, for example, the ACCC, the Australian Competition and Consumer Commission.

MS. DEUTSCH: Sure. I guess, you know, Verizon cooperates daily with law enforcement on a whole variety of matters, and we feel very strongly that we have to work to eliminate Internet fraud, both to protect innocent people, but also to bolster user's confidence in the Internet. In this case, the FTC's power to go after people flows from its police powers, and you do have I guess an administrative subpoena that you get to serve on service providers, and we're there to help you.

One of the cases that you've probably heard about that's garnered a lot of media attention, and that would I think actually result in more consumer fraud, is when that same police power to issue a subpoena comes from a private party, and that's been the case when the recording industry has sued Verizon, essentially that case would grant any private person the right to fill out a one-page form, send it to the service provider and get someone's identity, again, based on the same IP address that the FTC uses.

We're very concerned that this would actually result in more consumer fraud, because anyone will be able to get your identity, and at that point, if they want to perpetrate fraud on you, they have the key to

unlock your identity. So, we're very concerned with that issue.

That being said, I think there are some additional problems when the subpoena is coming from an agency outside the U.S.

Hugh, is that also your question?

MR. STEVENSON: Yes, it is.

MS. DEUTSCH: Okay.

MR. STEVENSON: And I apologize, I did not mention as a special guest star on the panel, we actually have one of the commissioners from the ACCC, Sitesh Bhojani, who also joined us yesterday, and maybe he then could comment on your comment.

MS. DEUTSCH: These are some of the problems that we've identified. I guess first of all, it's not clear that service providers have the authority to respond to a request from a provider or an agency outside the U.S. without some sort of mutual legal assistance, treaty or some other statute that requires that we comply.

I think right now in our own law, there's a provision in 18 USC 1703 that allows us to provide subscriber information in a law enforcement investigation for telemarketing law, but we don't think this extends to foreign law enforcement investigations,

because the way we see this defined in U.S. law is applying to only domestic agencies.

So, there's a question, I guess, as to whether we need a treaty and/or a statute in order to be able to comply more fully.

I think there's also a question about what is a fraud? We face this in the Council of Europe Cyber Crime Treaty that there are acts here in the U.S. that could be legal but are illegal overseas or vice versa.

For example, in Germany, comparative advertising is illegal, or Land's End offering a money-back guarantee for merchandise was considered an unfair marketing practice. So, you know, there needs to be some discussion of what would be a fraud, and I guess those are some of the main issues and we can get into the details later.

MR. STEVENSON: Okay. Commissioner Bhojani, maybe we could ask you to comment. Say we have the hypothetical of you needing to investigate a scam and needing to track back who is behind the website.

MR. BHOJANI: In an international context or in a domestic context?

MR. STEVENSON: I'm sorry, and let's assume that the web host or ISP you're dealing with is in the United States.

MR. BHOJANI: Yeah, that really has been -- we actually have experienced that sort of issue. It really has been relying on voluntary cooperation, I don't know that there is any power, I think what Sarah said is probably right, that there isn't any legal authority on which that sort of action can be undertaken. And so there is a little bit of an impediment in that sense, although we have had, as I say, some success just on a voluntary basis with various ISPs willing to provide that sort of information or whois database information as well.

What I'm curious to hear about is whether there is any grounds that Sarah thinks perhaps the fact that the commission, the ACCC may have instituted court proceedings in Australia might give you sufficiently or reasonable grounds to give us some of the information or to suspend services or things of that kind.

MR. STEVENSON: Sarah, do you want to respond?

MS. DEUTSCH: Yeah, I mean, I think we should clarify that if we get any request or alerting us of any fraud occurring somewhere on our system or network, we take a look and if we see something is wrong we try to do something about it, we'll either pull down the site or notify law enforcement.

So, we do want to cooperate, but I was kind of

looking at the bigger legal issues of what we would need in order to kind of create a more efficient process for dealing with some of these issues more globally.

MR. STEVENSON: Chris Bubb from AOL, maybe I could ask you for your sort of reaction to this, because I know that you all have had a lot of occasion to deal with requests from all over the world.

MR. BUBB: Yeah, we deal with international requests on a fairly irregular basis. Normally the international requests are based on the Mutual Legal Assistance Treaty process that's out there for criminal investigations. I mean, the actual name is misleading, it's not mutual legal assistance, it's mutual legal assistance in criminal investigations. So, it's limited to criminal context, but we do have a lot of relationships with investigations from other countries.

One of the things we've found is that it's often useful to use the [FBI] LEGAT in the embassies in the country that is requesting the information, where the FBI has LEGATS and there are other LEGATS in various embassies where they can act as an intermediary and get the information and then pass it on to the law enforcement or requesting agency and the requesting country.

Because the Mutual Legal Assistance Treaty process is a lot more efficient than it used to be, the

letters rogatory and the other processes that you had to go through were very cumbersome, but the MLAT is not exactly a model of efficiency in terms of dealing across borders, and countries are very jealous about their sovereignty and their jurisdiction, and they're not inclined to bend that at all, and that's why the mutual legal assistance is required.

I did some research in preparation for this and I actually found out that there are some interesting possibilities out there for action, I think the FTC has been a ground breaker in the antitrust investigations and have put together a regime called the International Antitrust Enforcement Assistance Act, and then they issue what they call antitrust mutual assistance agreements, bilateral agreements, because of this, they ran into the same problem, which was MLATs were criminal, and in many countries, the antitrust issues are civil and taken care of by civil authorities, and they couldn't get around the MLAT issue.

So, I think there may be a model there for dealing in a fraud context, to establish bilateral arrangements. It apparently has also happened in the securities and exchange, where they have identified, for instance a major fraud, and then they would engage in a memorandum of understanding between two countries for

the exchange of information under certain circumstances.

And I think that would be useful as a framework, or something like that might be useful as a framework for dealing with the civil law enforcement issues in the United States, and what we deal with mostly, which is I guess the back door, but the Australian issue, which is all of our information, or 99.9 percent of all the information that AOL has is resident in the United States, and all of our relationships with foreign law enforcement have been requests to us for information for a what we would call foreign or non-American request.

MR. STEVENSON: Chris, let me ask you a follow-up question on that, because I think the larger point is a very interesting one to us in the interest of looking in the securities and antitrust context for mutual assistance agreements, but let me, and I think Eric, maybe on your other slide, maybe this was clearer, these sort of timing challenges here.

MR. BUBB: Oh, absolutely, right.

MR. STEVENSON: And maybe if you could address that, and I have a weak grasp on this, but my understanding is the problem is that you got some of the information that you need to track back to the machine is just session IP address information, and so it's only good for a short period of time, and so if you don't get

it quickly, you sort of lose your chance to get the next step back in the chain.

MR. BUBB: Right. Absolutely. The issues are all generated by the magnitudes of scale that we deal with, at least in America Online. It's true of every Internet service provider within limits, but America Online is strictly based on a dynamic ISP. We assign an ISP to a user per session, and when the user relinquishes that IP, for whatever reason, whether he signed off or whatever, if he relinquishes that Internet protocol address that we have assigned him, that protocol address is available again for assignment to the next user.

We have 35 million members and the ability to have approximately three million simultaneous users. So, that means only one in ten people would, you know, at any given time be on, and so what we're talking about is a dynamic system, so it's temporal, it's time-based.

And we keep them for varying amounts of time, the information for varying amounts of time. We have emails, we deal with over a billion emails a day, over 13 million web hits a day. So, all of that information is collected and kept for varying periods of time, depending on the requirements of the company in terms of recordkeeping.

And so, we have retention issues in terms of that information. And it's extraordinarily important for law enforcement of any kind to come to us in a timely manner to get that, because it's sort of like Lucille Ball with the cherries going down the conveyer belt. You know it's going to fall off, it's going to drop, and no matter how hard Lucy tried to collect all the cherries, she couldn't do it, and nor can we.

There are some mechanisms that are very useful. There is a preservation request letter under 2703(f) where we will freeze that information in time and put it aside for law enforcement further requests, but even that has to be done in a timely fashion.

MR. STEVENSON: And let me follow up on that, because I think Eric or Lucy or Ricky or whoever told me that one of the challenges there is not the issue of getting you to preserve it, it's sort of to get the entity behind that to preserve it. And actually, Eric, if you want to just mention what we had sort of discussed about your concern there.

MR. WENGER: Sometimes what happens is that there's an Internet service provider and then they use somebody else to provide telephone connectivity, and for instance I think AOL has companies that provide the modems in each of the cities, and so we need you to

preserve the information you have and then also there's a challenge of getting it back quickly enough in order to get a preservation request to whoever is providing that actual modem.

MR. BUBB: Right. All of AOL's dial-up operations are contracted out to one of five or six dial-up providers, including WorldCom, Sprint, companies like that. And you're absolutely right, that the only chance you have of getting to the actual, in your scenario, the user location, the telephone or the home that it's coming out of, would be a two-step process with America Online, to get our information and then to get the information that we have that leads back to the dial-up provider.

We do that, and as a matter of fact, interestingly enough, when we do it, when we provide the information back again, we give a cheat sheet along with it, as well as the whois information for the dial-up provider and the contact telephone number. So --

MR. WENGER: I guess I'll put this out to any of the Internet service providers. If there's a situation where there may be somebody downstream from you that we may need to get information from, would it be possible for us to give you a preservation letter that would cascade, in other words you would send it immediately to

the secondary preservation, in other words, we wouldn't have to wait to get back your information and then get a second subpoena.

MR. STEVENSON: Another way of thinking that, on a voluntary basis, is there a way to get at least so the information is preserved immediately, even if it can't be obtained immediately?

MR. WENGER: We would of course have to issue the subpoenas to both companies to get the information. But if it would turn out by the process of issuing the subpoena and getting a response from the first company would take so long that the second company would no longer have the data, the question is exactly as you put it, is there a way to preserve everything downstream, just preserve the status quo in a way that allows us to in the course of time issue the subpoenas and get the information.

MR. BUBB: Well, I guess it wouldn't be a problem, the only practical observation I make about that is that when we process the information, that's when we know who the downstream provider is. So, we wouldn't know it until we process it. So, we wouldn't be able to say that it was UUNet or Sprint or Genuity.

So, it adds a complication to it. I hadn't thought about it, I don't imagine there's a huge issue.

What we could do informally is to notify the downstream provider that we had gotten the request, and ask them to take the steps they need to take relative to it on an informal basis. I don't think we would do it formally. I mean, we would ask for it, because I don't think we would be, I don't know, I guess I don't know what the legal term would be, but really in a position to demand that they do it, but I don't have a problem with an informal request saying that we had gotten this, it's connected to you, would you look to preserve.

Or the other thing would be as soon as you get the information, I mean you would get it roughly about the time that we got it, immediately issue a request for preservation to them. Our dial-up information, I guess on the other side of it, is among the more durable records that we have. It's the longest one, amongst the longest retention tables that we have. But that's a side issue.

MR. STEVENSON: I don't know whether Sarah or Kristen wanted to reply to that particular point.

MS. DEUTSCH: I mean, for us it's a very relatively small ISP compared to America Online. We're also not a backbone provider. I think the issue will come mostly for the backbone providers and the key here would be getting you enough information as quickly as

possible so you know who this downstream provider is and you can get this request to them as soon as possible.

MS. VERDERAME: If I answer this question, it opens a whole host of other issues that I am not going to get into at the moment. In the European system, it's quite different from over here in many respects. One of the issues is that privacy over there is actually a human right, so it's very highly protected. The data regime over there is very severe and very strict. So, any kind of disclosure, whether it's to law enforcement or anyone, is severely limited.

The European data protection directive under which we have to work also requires mandatory destruction of data. So, if you're talking about going in and wanting to find certain information that's there, if it's already been destroyed, there's an issue.

In direct answer to your question, what I would say is that we have very good relationships with the ISPs that we serve through our content hosting business, and also as an ISP with our customers. We have contracts that cover this exact type of situation, if an issue arises, we can terminate service immediately, with no notice. We work very closely with law enforcement and are happy to work, even on an informal basis, contacting the ISP with whom we're serving through our

content hosting business, or the customer directly or whoever it might be, downstream, to try to preserve information.

If there's no legal requirement to do so, we can't force their hand, but we have been known in the past to do that, to work cooperatively with folks to try and preserve what law enforcement is interested in seeing.

MR. STEVENSON: Kristen, let me just pose the scenario, maybe this is the reverse of the one we were talking about earlier where the -- say the Australian consumer protection folks are trying to get information from an American web hoster ISP, and so the sort of different scenario is say where the FTC or the ACCC is trying to get information from a European-based ISP. I mean, how does that look in terms of your ability to respond? Is your answer different from Chris', or how is it different? Obviously you've suggested already it's different.

MS. VERDERAME: It's not different as far as legal procedure goes. We have the same concerns as far as desiring some sort of international treaty to give the entity the authority to come in and get that information from us, but we also have to overcome the data protection restrictions and requirements that we

have to fulfill there. We certainly have an expert on the panel who can speak to that more than I, but that is a definite hurdle that we have to overcome is the data protection regime.

MR. STEVENSON: Eric, I think you had a comment following up on that.

MR. WENGER: The flip side to the scenario that I proposed before is where, for instance, there's a web hosting company that gives me back and I give him a subpoena and they have an IP address that comes back to one of the ISPs on the panel here. Would they be willing to accept a confidentiality request that comes upstream from you, absent -- in order to avoid the situation where I have to, again, wait for the response to come back from that other company, and then issue a preservation letter to you during which time the data that I'm looking for might evaporate?

MR. STEVENSON: And Eric, maybe it's helpful for you to talk about the time frames that you've encountered in terms of how fast you need the information.

MR. WENGER: For example, in something that I'm currently working on, there was a web hosting company that gave me -- I issued a subpoena, it takes about two weeks from the date that we have a subpoena issued for

the responses to come back, and then I get back an IP address from them that comes back to a particular Internet service provider. And I say to them, I want to know which of your users was assigned to this IP address at this date and time. And they tell me that their record retention is only for about seven days.

So, the process of just the response time for my subpoena exceeds the length of time that the data is retained for. And I understand the sensitivity, I think we all do at the FTC, about just having data retained forever, because there are cost concerns and there are privacy concerns, but our concern is that where we have narrowly targeted requests for information, that it be retained and disclosed, are there ways to make sure that the information is there when we need it?

MS. DEUTSCH: Well, I think you've got a very legitimate concern. I mean, Verizon keeps the session logs for a very long time. I mean, months, you know, in some cases years later you can get from us, you know, the user ID, their phone number, address, the date and time stamp that this was happening. I think we need to push for some best practices so that these kinds of records can be kept in a manner in accordance with the usual business practices that also, you know, serves the needs of the law enforcement community, but that's that

we feel strongly that it's still preserved.

We would prefer a data preservation model versus a retention model, but for these types of business records, I think we should, you know, try to work toward better practices so that you can get the information you need.

MR. STEVENSON: Is it fair to say that the -- because one issue we've heard raised in many larger contexts of obviously it's a burden of retaining just this information in general for a long time. Is it fair to say that to the extent there could be developed a mechanism for targeting smaller amounts of information to be preserved, that that is maybe a useful direction to go in terms of our ability to investigate these cases?

MR. BUBB: I think that's exactly the model that's preferred. Just again, I always like to view these things in context, and one of the contexts is in some of the dynamic IP addresses that we deal with, and I won't go into the technical ones, but one set of servers at America Online generates between seven and nine tarabytes a day of information relative to certain IP addresses. I mean, that's just an enormous amount of information to preserve to hold onto. And it starts to -- the answers to the questions that are posed start

to be practical answers rather than, you know, sort of theoretical answers.

The practical answer is there's only a certain amount of space that you have to store between seven and nine tarabytes, you know, we're having to learn whole new vocabularies of the next thing up from a tarabyte. So you're really starting to look at massive amounts of information. And we preserve actually a lot of it.

I think the second thing that needs to be observed is that there are two things. One is the information, the second one is the ability to resolve that information down to an individual user. And a lot of times, at AOL, we go out of our way, and it's a part of our own business, not in order to assist anybody, but we retain the ability to resolve it down to individual users over time. A lot of times, there are vast amounts of information that are kept and logged, but they are not able to be useful to any law enforcement agency that would come to you, because they're just a mass table of IP addresses.

So, that's a secondary thing that one has to keep in mind with web hosting or anything else is whether that information that is kept is capable of being tied to anybody, to being resolved back to or pointing to anybody.

So, that's just a secondary issue.

MR. STEVENSON: Okay. Thank you.

Well, and so both the challenge is to tie it to someone, but then that also raises some of the privacy concerns that Kristen raised. I guess I would turn next to Jonathan Bamford and ask is Kristen's assessment basically correct, then, and how should one look at this? How can one get this done consistent with privacy concerns?

MR. BAMFORD: Well, Kristen is not far off the mark in terms of the fact that you do need to be concerned about data collection legislation, and perhaps because perhaps we are two nations divided by a common line, I ought to actually explain what data protection legislation is, because it's not some overarching absolute right of privacy.

It is based on, to a certain extent, the European Convention of Human Rights and individual rights to a private life, but even that is not an absolute right and that can be interfered with certain circumstances in accordance with the law and in a proportionate manner to the evil you're trying to address there.

So, clearly, there's a balanced approach in a sense of respecting people's private lives, and actually

protecting the States against criminality over individuals against criminality against them. Or of the fraudulent activities. So, it isn't an absolute right.

I mean, in common with many, many other countries around the world, not just European Union countries, but Canada and Australia also have data protection legislation that sets down some legally enforceable standards in terms of the collection of the information. Most individuals understand when they're providing information, how it's used, how it's disclosed, data quality standards regarding accuracy and the things that have been searched done elsewhere and searches as far as the accuracy of data and also security.

The thing I would stress to you is that data protection legislation only actually relates to identifiable living individuals. There's no protection for companies or anything like that. Or aggregated data or anything along those lines, it's only where it actually points to an identifiable living individual.

And I think it's important to understand as well that it does apply to both public and private sectors in most jurisdictions as well. It also provides some protection for individuals as well in terms of rights to access and things like that, which perhaps we don't need

to go into today. And also one key feature of the data protection legislation is that you have to have an independent supervisory authority, and that's the Information Commission of the United Kingdom and all jurisdictions have their own supervisory authorities.

And we try and work in a constructive way to deal with the very issues that you're raising there, Hugh, in terms of providing people with the appropriate advice in terms of how data protection legislation applies. And sometimes there is the immediate reaction that, hah, data protection legislation applies to some information about some individual that's being sought here, therefore you can't have it. That would be a wrong approach to adopt.

Data protection legislation usually has certain balancing features in it. Indeed, sometimes you can disclose information just because you've made people aware at the time that they signed up to be your customer, how you are going to use and disclose their information. Not particularly relevant when we talk about whois databases in certain instances and relationships with ISPs in terms of how widely that may be made available, indeed to the law enforcement community, in its wider sense.

But a lot of the questions that you've got to

ask in data protection terms is centered on the nature of the data being sought. I think there were some relevant questions starting to be posed yesterday that were described as meta data, but what actually we are talking about sharing here, although I have to say I'm not quite certain it's alway sharing as a disclosure of information, it's giving information. Sort of my kids' definition of sharing I think is probably used, actually. But they get everything and never share it with their sisters.

But, basically, you know, it's a question of what's being sought. And there's clearly differences there between an actual investigation into somebody who is a suspected perpetrator of a crime and perhaps other information which is generally about customers to help identify crimes, trends or other things which may suggest they have been subjects of the crime where actually they haven't done anything wrong and there's different responsibilities there.

Within our data protection laws, we often have exemptions from what we call our nondisclosure provisions, which restrict disclosure, where failure to disclose would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders. There are some issues on the merging of

what's an offense and what's not an offense, but there's a mechanism there, our policing in the UK hasn't simply grounded to a halt since we've had data protection legislation since 1984.

They can find out information about people because they request it on the basis of its likely to prejudice the prevention or detection of crime, and people then faced with that request, whether it be my Internet service provider, who happens to be BT Internet by some chance there, and but, you know, they would weigh a question in terms of would it be -- do they have reasonable grounds for believing it likely to prejudice crime prevention purposes.

Similarly, if they're under a legal compulsion to provide legal information as a result of a court order or some direct legal power, they can do that without violating data protection laws. There's wider issues we're touching on here about the applicability and the legally binding nature of a court's orders from other jurisdictions or other powers of body there, which maybe we'll come back to, but there are mechanisms in legislation which permits disclosure in certain circumstances.

MR. STEVENSON: Let me ask you in terms of the scenario of one issue in response to a legal process,

but for example, take my scenario where the ACCC is investigating somebody who needs to go to British Telecom to get information. Does that pose a problem?

MR. BAMFORD: Well, the first instance, if I was in British Telecom's shoes, I would be asking who the heck are the ACCC, which might not be actually be known to many people. No disrespect there. And perhaps other people in the UK that would ask that of the FTC as well because they wouldn't know. I'm sure you're very, very well known over here, but we don't know who we're dealing with in many instances. If you're in that position.

So, how do you know that it's a legitimate request from a law enforcement agency? And that's the real difficulty. I don't know how somebody would react if they got a request from the Hazzard County Police Department, I don't know whether that's a legitimate police force or not.

It's difficult. And I would actually say a better model, and we're here talking about partnerships in the title of this conference, is to have a designated contact point within that jurisdiction with the appropriate powers. It's the conduit of finding the information, because the people locally are used to dealing with those, they know them as a law enforcement

agency, and they can be the appropriate conduit back.

Within the UK, we're doing things to try, it tends to be in the criminal law areas, but we have a bill going through Parliament at the moment which is essentially a crime international cooperation bill, which is all about one serving process, clearly people's responsibilities in terms of obeying, that's a rather difference in a jurisdiction where you can't enforce it, but two, assist in investigations to provide the necessary information.

So, we're trying to bring about a system of greater cooperation. That brought to bear in the data protection context, if a local law enforcement agency perhaps has requirements for somebody to provide something, such as our Office of Fair Trading, then that would be the conduit back.

And I would make the point as well, that presumably because we're talking about the Internet here, and therefore the crime can be committed against consumers anywhere in the world, there may be well some local jurisdictional issues as well, if the suspects are operating in the UK, that they are actually committing crimes against UK consumers and they have a legitimate law enforcement interest of their own, which again gives greater weight to a disclosure by an ISP based in the

UK. It's a local law enforcement concern.

MR. STEVENSON: Let me follow up on two things there. One, I wanted to see if I understood correctly one of your suggestions, which is that the ISPs may be able to address some of the privacy concerns in terms of service, in terms of disclosure of what might be done with the information? Was that one?

MR. BAMFORD: It's a possibility of doing that. I mean, I think it would depend on the nature of the data and whether there would be some unfairness to individuals. Clearly when there's a situation where there's a complete legitimate concern about somebody, you know, and there's real issues about their compliance with the law, you perhaps are less dutious to them in terms of fairness and how you process their information, than you would about people who are potentially completely blameless.

And so it would depend upon the nature of the data that's being sought, the extent to which you could rely on a contractual term, but it's not so unusual as you will see when we talk about whois, to see in contractual terms the fact that this information will be disclosed to bona fide law enforcement agencies.

And I think you'll all find as well as a result of an agreement between the EU and American authorities,

airline passengers are being told how their information will be available to U.S. authorities, and now if you read USA Today on that particular agreement.

MR. STEVENSON: I think that's an interesting point to think about. The other issue that you raised, Jonathan, was the issue of working through the local authority, the local enforcement authorities, local from the point of view from I guess the ISP or the web hosting company, and I'm wondering whether anyone had any reaction to that. Does that make sense to -- maybe the better way is to say, that makes sense, doesn't it? Or is there a particular reaction? Or is there a different model?

MS. VERDERAME: Well, I would add that that is correct, and that's the method that BT certainly uses. That's sort of our first port of call.

If I could just make a couple of comments. First of all, I would say that earlier my intention in stating or raising the data protection regime was not to say that it prevents us from disclosing information to law enforcement and that sort of thing, just to strike the difference between the U.S. and the UK. We don't have that over here, we do have that to think about that over there. In fact, when I surveyed a lot of our folks with questions for this panel, one of the first things

out of their mouth was data protection, we have to think about that first.

So, we're actually grateful to have the information commissioner's office to go to when there is an ambiguous area. Certainly we have a process in place, when things come in the door, we have people dedicated to look at the subpoenas or whatever they might be, they're familiar with the ACCC and other authorities around the world, so we have a process in place and it does include, in fact, law enforcement on that.

MR. STEVENSON: Thank you. I would like to turn now to Cedric and ask for his reaction as someone who focuses on privacy issues and I'm wondering whether the scenarios that we've described and that Eric described, what kinds of issues that raises from your point of view, what concerns, what ways are there of addressing them?

MR. LAURANT: I would like first to re-focus the debate a little bit, because so far, we've talked about how data protection, how privacy laws may be hurdled to law enforcement work, and especially the law enforcement work of the FTC. But I would like to remind you that the FTC is, first and foremost, a consumer protection organization whose main task is to protect consumers

from fraud, from identity theft, et cetera.

The second point I would like to make is that law enforcement has its own interest in, for example, suing criminals, suing identity thieves, et cetera, and then consumers have privacy interests. So, you have to take into account on the one side, law enforcement interests, and on the other side, privacy interests.

We at EPIC, Electronic Privacy Information Center, of course are more focused on privacy issues and on protecting, on raising labor issues and price issues and trying to understand how consumers can get their privacy better protected. And I think that the role of the FTC as a consumer protection agency is to take into account in balancing the interests of, on one side, law enforcement interests, and on the other side, privacy interests. And having this framework in mind, I think we should think about, because we are on a panel trying to understand how law enforcement and private sector could better cooperate among each other, with each other.

I think we should try to understand why there may be impediments to the sharing of information. Those impediments probably exist between, for example, the United States and the European Union, because the European Union promotes data protection as a human right

that is protected by the European -- mainly by the European Convention on Human Rights, in its article 8.

And taking this into account, a way to have better partnership between a private and law enforcement and public agencies would be to have kind of general framework, general data protection framework that could be incorporated into the various memoranda of understanding or intellectual agreements that are now being signed between countries like Australia and the U.S., United Kingdom and the U.S., and Great Britain and the U.S., and such a framework could actually be the OECD privacy guidelines, so the Organization for Economic Corporation and Development privacy guidelines.

Let me remind you that the FTC has always been very active, first of all, in drafting these guidelines, and then in recognizing them as a good model to protect consumers, especially through the fair information practices.

So, we at EPIC would view the OECD privacy guidelines as a good supernatural framework to protect consumers' privacy, and we think that it should be incorporated into the various international agreements that would promote better cooperation between law enforcement authorities and private companies, and consumer agencies.

MR. STEVENSON: Thank you.

Let me follow up on part of that comment. Obviously one of the things that needs to be addressed is some understanding across borders of how these things might work. There is an Australian example, and maybe I could ask Mr. Bhojani to address, but I think it's particularly the ASIC, sort of the Australian version of the SEC, has been involved with in terms of voluntary codes with the ISPs. It's just sort of an interesting project that perhaps if I could ask you to just describe that briefly and ask whether that has the potential of broader applicability.

MR. BHOJANI: Thank you, Hugh.

Yes, if I could put the issue in a bit of a context, most of you, I think, have probably had a handout given to you about the sort of Australian Communications Authority, which is not us, obviously, but one of our sister agencies who's responsible in this area, have put out on Internet service providers and law enforcement in national security.

That sets out the sort of legislative basis, and actually has an obligation. If you happen to look at the first page on ISPs, to actually give officers and authorities of the commonwealth assistance in relation to enforcement of criminal laws, laws imposing pecuniary

penalties, protecting public revenue and safeguarding national security, and to do their best to prevent their networks and facilities being used against the commission of offenses against the commonwealth and the states and territories in Australia.

A couple of other interesting aspects of that, because I think somebody in this panel or the last panel was also concerned about the risks of being sued for inappropriate disclosure. And under section 313 of the Telecommunications Act of Australia, it provides that a carrier is not liable for damages for an act done or omitted in good faith to give reasonably necessary assistance to officers or authorities of the commonwealth states and territories.

So, there's an expression provision that absolves the ISP from liability for the things done in good faith to assist law enforcement agencies. But that's the statutory context. And what Hugh's question was really directed to was the voluntary process beyond that, and in Australia, we have the Internet industry, which has got together with a number of law enforcement agencies to create what's now known as the Internet Industry and Law Enforcement Agencies Cyber Crime Code of Practice.

It's available for those of you that want to

have a look at this, in terms of the details of it, at www.iia, the Internet Industry Association, so iia.net.au. The code recognizes a common interest between the industry and government in prevention, detection and investigation of online fraud to foster user confidence. It confines itself to the cooperation between ISPs and law enforcement agencies, but does allow for future extension to hosting and e-commerce.

Under the code, ISPs are required to keep, this is a voluntary code, not a mandatory code, but a voluntary code, and under that code, ISPs are required to keep the name, address, phone numbers, credit card details and billing info of customers personal data, for at least six months after a person ceases being a customer, and dynamic IP allocation records and customer log-out times and dates, what they refer to as operational data, for at least one year after the date of creation of the data.

Now, that code, it remains to be seen how workable it is and how it's used in the future, but one aspect of it that does potentially cause some problems is the concept of interception. ISPs, many of the law enforcement agencies don't have interception warrant powers. There's no ability, for example, for the ACCC in Australia to be able to get a warrant to intercept

telecommunications services or Internet services.

Interception in Australia has caused a little bit of a problem, because recent legislative amendments to obtaining information were proposed as part of the anti-terrorism practice by the Australian Attorney General's Office, and those amendments sought to redefine, to an extent, when an email had been received.

So, when is something actually received, as meaning when the addressee opened it on their PC, rather than when it was received by the sender's server or the service provider or other intermediaries, or the recipient's service provider or the recipient's server or the recipient's PC. It was being redefined to when the recipient actually opened the email.

Now, although there were differing opinions in Australia about the effect of that, there was a real concern by law enforcement agencies that it had the potential to stop them from obtaining any unopened emails from suspect PCs without a specific type of telecommunications interception warrant, like a wire tap provision.

And the ACCC and other agencies, as I say, do not have that ability, due to the concerns that we have raised, that aspect of the package, the anti-terrorism package, has been shelved, and it's been ordered to have

a further review in terms of our interception act provisions. But they're the sort of technical issues that are going to arise in some of this sort of information in terms of interception, but I think that code certainly does have the potential to provide a global sort of informal process, voluntary process, but I would be very interested to hear from some of the firms here as to whether it's sort of achievable in the volumes that we're dealing with that we were hearing about earlier. Those sort of time frames, whether they're realistic or not.

MR. BAMFORD: Just a few words following up on that in terms of mandatory retention periods. In the UK, we've recently introduced an antiterrorism crime and security act. One of the elements in that deals with the retention of communications data which will cover traffic through an ISP, and the mechanism there is to put in place some requirements to retain data for longer than would be necessary for the ordinary business purposes of the communications services provider in question.

To say from a data protection point of view, our laws, which I touched on earlier, do require that personal data is held no longer than necessary for the purpose, and if your purpose is various

communications over the Internet, so your business purpose then is the retention period that's set. This is a way of preserving it for longer.

In the UK when these provisions went into Parliament as a bill and the provisions to retain the data was expressed in ways that it could be retained for a period of time for any criminal matter, but actually as a result of scrutiny going through Parliament and general concern, that actually changed to say that the data that's retained can only be used for national security purposes, i.e. to deal with things that do touch on terrorism and not things that might be of a serious nature in other ways, but not actually of that serious nature, and we have a strange concept of a code of practices part of this as well, but it shows that we adopt a much more measured approach to the idea of retention of that sort of data linked to a real pressing need and harm, which in that case is terrorism.

MR. STEVENSON: I take it there you're focusing on the provisions that are more system-wide as opposed to the scenario, for example, that Eric proposed of it given that you have a given case and a given investigation and preserving information in relation to that given matter.

MR. BAMFORD: Well, there's no actual mechanism

for any preservation as such in the UK context. In some ways, that would be more privacy friendly. The general retention of records for a period of, say, up to a year with respect to any pressing need, so in some ways, preservation of an actual problem is a better solution in privacy terms than one which is a blanket retention of data of all of a particular period in time. We don't really have that provision.

MR. STEVENSON: Would you agree with that, Cedric?

MR. LAURANT: Actually let me quote a recent report that was released about one month ago, I think, by a British Parliamentary company. This report shows that a one-year data retention scheme if implemented would be impractical, the costs have been underestimated, and the Internet service provider and the data communications industry have had so far few incentives to implement any technical changes, not to mention the fact, also, that the retention scheme appears to be in breach of the United Kingdom human rights legislation, which implements the European Convention on Human Rights.

MR. STEVENSON: Thank you.

The other issue I would like to turn to, quickly, and then if there's some questions I would like

to take those, is the scenario of suppose we've done the investigation that Eric was able to get the information, and the commission has pursued an action, then what happens then?

MR. WENGER: Well, what happens then is we typically will, for instance, if we're dealing with somebody who we don't think will respect an order that we serve upon them to stop, we will get a court order that we serve upon registrars or web hosting companies asking them to take down the content that we feel is violative of the Federal Trade Commission Act.

And we've had, especially in the international context, difficulty in doing that. And so I wanted to raise for you that issue about whether or not you would respect orders that are coming from foreign courts, are there voluntary mechanisms for notifying you about fraud that you would respond to, those sorts of questions.

MR. STEVENSON: Maybe if I could ask Chris and then Kristen, do you have any response on that?

MR. BUBB: Well, we've had a lot of requests in dealing with requests for taking down information on the basis of violations of our terms of service. If you come to us with an order that reflects a behavior that is violative of our terms of service, we'll take them -- we'll take them off the service, and that has as much to

do with the fact that I think our terms of service are at least as restrictive and I guess the short version is we don't want this stuff on our service.

If somebody is being defrauded or somebody is being injured in some way or if somebody is using a name that is deceptive or using a practice that is deceptive, we don't want them on our service. We're not a big web hosting service, but if they certainly impact AOL we'll take them down. And it's not so much in terms of the fine points of jurisdiction or sovereignty, it has more to do with the fact that we look at it on our service, we don't want it there. So, it's consistent with that.

MS. VERDERAME: Yeah, I would agree with that. We have pretty much the same procedure. And building on a point that was made earlier with regard to consent, that is one of the exceptions for data protection rules. So, we have, in fact, built into all of our contracts in contract hosting limitations on use. If we find out that a user or customer is using web hosting services in any way that is fraudulent or unlawful, we word that extremely broadly on purpose, we have the right to immediately terminate the service, and we, in fact, do that, if we receive a request or a complaint that's substantiated.

We also build it into contracts that we have

with our ISP business. We notify customers in our privacy policies all over the company, whether it's retail customers, whether it's content hosting, whether it's business service customers, we specifically say in our privacy policy, if you break the law, if you use our services to break the law or do anything fraudulent, we will give your information over to law enforcement if it's legitimately requested.

So, we do install that into our practices and procedures based in part on the data protection regime that we have to work with. But I think it's the same procedure that AOL follows as well.

MR. STEVENSON: Thank you. We have time for a couple of questions, if there are some. If people have questions or comments that they want to address to the panel. We have one here.

MS. KLEIMAN: Kathryn Kleiman for the Association of Computing Machineries Internet Governance Project. A question for Mr. Bhojani, I hope I pronounced that correctly. The law that you cited in Australia, that enables cooperation between say the ISPs and registrars and law enforcement. What does that do in the situation where ISPs and registrars are contacted directly by foreign law enforcement? Let me give you two scenarios, please.

One scenario would be being contacted by the Federal Trade Commission of the United States, regarding a fraud investigation. Are the registrars and ISPs free to cooperate and are they free of liability if they do?

The second question is what if they're contacted by the Chinese government regarding a domain name that's being used for pro democracy, anti-Chinese information? Same thing, do they hand the information over? Do they notify the registrant? Do they cooperate? Are they free of liability, if they do?

MR. BHOJANI: Thank you. Unfortunately, the laws that we're talking about really are focused on laws of the commonwealth of Australia. So, really it's protecting the ISPs insofar as they're assisting law enforcement agencies at a domestic level, rather than on the international level.

It would still be a requirement, I suspect, in terms of the dialogue we've been having here, that most of the ISPs would want to see a court order before they would touch anything in an international context.

MS. KLEIMAN: An Australian court order?

MR. BHOJANI: Well, a foreign court order that they would be willing to recognize that they are somehow absolved of liability. The liability provision that I was referring to was, again, protecting them from

liability where they act in good faith to assist Australian law enforcement agencies, rather than international law enforcement agencies.

The point that Kristen made and others have made as well, the ability to work through local agencies in that context, it might be that the FTC would come to the ACCC to try to get assistance from us, or the Chinese government would do likewise. And we might be able to see whether there's something that breaches our law that we might be able to go to the ISP with as well. And that combined might be able to achieve an outcome that a direct approach may not be able to achieve.

MS. DEUTSCH: Kathy, I just wanted to give you a real example from Australia that I just read about two days ago. The members of the recording industry have demanded from the universities, who are also ISPs, that they turn over essentially all of their traffic data on their networks to the recording industry companies so that they can scan this information for their own purposes.

MS. KLEIMAN: Has there been any response?

MS. DEUTSCH: I think that the universities have the data but they haven't yet said what they are going to do.

MR. STEVENSON: Alistair, did you have a

question?

MR. TEMPEST: Thank you very much. Excuse me, because I missed yesterday for various snowy reasons, and it may well have come up yesterday, but I thought it was a point which has been raised just now and which Sarah raised right at the beginning of this panel, which I think is very important. That is, the application of national laws as compared to the application of actions against criminals. I think there is actually a very big difference.

When, for example, someone breaks a law which creates fraud, that is something which I think nearly everyone can accept across the world. Because there is a damage to an individual or whatever it happens to be. The issues that we start to look into here, particularly on things like data protection or the issue which was just raised where someone has broken the law in China, and someone is being asked in Australia to apply that Chinese law is something a lot different and creates a major problem.

There is, of course, the Hague Convention which is going on at the moment. In Europe we have an issue, and a very live debate about three conventions on jurisdiction, and where that jurisdiction should be applied, should it be applied in the country of

destination, or the country of origin. And I think that is an area which, perhaps, there will not be such an easy international agreement as some of the other discussions we've had today, but I don't know what the other panelists feel.

MR. BAMFORD: It's partially touching on the point that you raise in there, Alistair, which I mean, some of those are bigger issues than anyone in this room can decide, I suspect. But if we come down to sort of practicality in terms of the information and sharing end of things and the information disclosure end of things, I think when you're actually talking about what's the appropriate data to share, you know, we do need to manifest this in some sort of memorandum of understanding, information sharing protocol between appropriate agencies to give people confidence that actually the information that's being shared is for things which would be legitimate concerns in both countries in terms of it being related to the loss and not the Chinese example or Iraqi example or anything else you might want to bring forward which might not be absolutely coterminous with an offense in any of our particular countries, but I think as well it's an opportunity, and I think Cedric was touching on this as well, to put in place something which sets the

boundaries then in terms of what can happen with the information.

Because I know from a data protection point of view, one of the things that does worry us is that when somebody provides information initially for bona fide reasons, once that's gone to somebody else, what's the ring fence that's being applied on it being used in any other ways? And we've had this with disclosures to U.S. authorities in the past, well, I shouldn't say European police office, Europol, for terrorism. When we looked at essentially the number of people who could have access to this, it was 20 some thousand U.S. enforcement authorities.

We sort of a differ a little bit at that point from a European perspective, there is a very, very wide disclosure that's going to take place, information sharing agreements, protocols, perhaps can start to set some of the boundaries of reassurance there, how long the data is held for, those sorts of reassuring points there, and indeed mechanisms, and this came up yesterday, to make sure that if the data changes and the finger of suspicion has been lifted from somebody, then that information gets passed on as well to make sure that records are kept up to date.

And we have plenty of experience in the UK of

multi-agency approaches to information sharing where people don't really deal with it in a very professional way and there's all sorts of impacts on people's private lives as a result of that. I would worry about that in the international context.

MR. STEVENSON: Any other questions? Eric?

MR. WENGER: Two things I wanted to point out. With reference to the point that Cedric made about the need for information, I think it's an excellent point. And I think at the FTC we're especially cognizant of the balance between privacy and law enforcement. And the scenario that I posed was actually assuming that we found something that was fraudulent that we believed needed to be investigated, but I think particularly here where we are a regulator that enforces laws that relate to privacy and also have worked hard to promote privacy in the private industry, that that is a point that we're very aware of and cognizant of.

Also, I think we're also very cognizant of the costs that are associated with preserving data for open-ended periods of time. And so we do understand those concerns. And finally, I wanted to take up the challenge that was raised by Commissioner Swindle in the first place about talking about the good as well as the bad.

And I think that I wanted to make sure that everybody understands that we actually have had very positive experiences dealing with Internet companies that have set up special contacts for us when we're conducting investigations that we can reach out to, that have allowed us to use fax or email ways to communicate with them to speed up the time frames and get information back in response to our subpoenas quickly, and who have preserved data upon request and in response to our subpoenas, turned that data over to us in timely ways. And the ability for us to get that information has been vital to our success in fighting Internet fraud.

MR. STEVENSON: Thank you. Eric, and I wanted to adjust one point in response to the issue that Alistair raised about the jurisdiction and conflicts of law. I think there are obviously very great difficulties that go on in a lot of those issues, and it is a challenge, and I think one of the reasons that we in the OECD, Commissioner Thompson is describing, our joint work there on cooperation to address cross-border fraud and deception, and one of the challenges there is we were picking an area where, as Alistair suggested, there is some common understanding of an area where the conduct is problematic, no matter where it's occurring,

and frankly even then, we have a lot of challenges as we hear and how do we best cooperate, but the idea is to focus on precisely that kind of conduct and develop these connections so that we can make progress forward.

We have run out of time, and the press conference will be here in just a few minutes, then we will start back up at 2:15 sharp with our panel on domain name registrars, so I will end by thanking our panelists for what I thought was an excellent discussion. Thank you very much.

(Applause.)

(Whereupon, at 12:45 p.m., a lunch recess was taken.)

AFTERNOON SESSION

(2:15 p.m.)

MS. MITHAL: Okay, why don't we get started.

My name is Maneesha Mithal and I am the Assistant Director for International Consumer Protection here at the Federal Trade Commission and I would like to welcome all of you to this panel on cooperation between consumer protection enforcement agencies and domain registrars and registries.

As you can see, we have a very large panel today, and it's actually a fairly long panel and we're hoping to cover many issues, but I thought it might be useful to start by just setting some ground rules so that we can streamline the discussion.

The format of this will be moderated discussion, so I will just throw out issues and questions. When you would like to respond or if you would like to respond to another panelist, just please raise your tent and wait to be called on by me. This part is very important, I would just ask that all of the panelists keep their remarks as short and succinct as possible, and as to the point as possible.

I promise you that if we all adhere to that rule, everyone will have multiple opportunities to speak. And I just want to give you fair warning that,

you know, we do have a lot of issues to cover, and please don't be offended if I ask you to move along or finish your points.

So, to that end, I thought it would also be helpful if we divided up the panel into segments. I thought we would spend the first half hour or so talking about whois data in the generic, top-level domains. I thought we would spend the second half hour or so talking about whois data in the counsel domains, and then we can take a short break and talk about information sharing generally between consumer protection enforcement agencies and domain registrars and registries.

And then finally spending about a half hour or so talking about how we can suspend fraudulent websites and how we can work together on that. And this panel should wrap up right around 4:30 or so and we should have an opportunity for people from the audience to ask questions.

So, let me also just start by defining some terms here. I think most of you are familiar with them, but for the benefit of those of you who haven't, we'll be using the term "whois" a lot. Whois refers to a set of databases where domain registrants' contact information can be found.

We'll be saying the word GTLDs quite a bit. GTLDs refers to generic top level domains, those are domain names ending in .com, .org, .net, .info, .bus and some others. And those domains are generally regulated under contracts ICANN or the Internet Contact for Assigned Names and Numbers.

And then we'll be talking to you about CCTLDs quite a bit and those are country code top-level domains and those are domain names ending in two letter country codes, like .UK or .GE for Germany.

So, with that, why don't we jump right into it. I thought it might be useful to set the stage a little bit, and so I want to ask Dan Salsburg from the FTC to talk a little bit about how we use the whois database in our investigations.

MR. SALSBURG: The whois database or databases really are the first steps we take in most of our Internet fraud investigations using these databases. We routinely go to the databases to find out who is responsible for the given website, the name of the registrant. We try to find out from whois databases the identity of the registrar who can be served with process and we can make requests upon for additional information.

We look at the address information that shows up

in whois listings to determine where is this business located. We look at the host information to find out where the servers are located. In short, without whois, we have a very difficult time finding out who has responsibility for a website that may have some fraudulent claims on it.

We also use the whois database in another area, and that is oftentimes, in addition to the work we do stopping frauds, we engage in what are called surf days, which are designed to identify the prevalence of fraud or activities that appear that they may have fraudulent components, and inform the purveyors of those websites of the problems with their websites and ask them to respond.

For instance, often we will get together with state attorneys general or with our counterpart consumer protection agencies with other countries and we will review numerous websites, if we find problems with websites we will send emails to the people or the email addresses that show up in the whois database under the contact information and try to inform them of the problems that we saw with the website.

MS. MITHAL: Dan, can I just follow up. Could you lay out some of the -- do we face any concerns with the whois database right now?

MR. SALSBURG: Yeah, there are a number of problems, but the two principal ones are first of all the accuracy of the data in the whois database. We have seen in one case we had there was a registrant that was engaged in some pornographic commerce, and it happened to be listed in his whois entry as being located on Foreskin Street in Amsterdam with Amanda Huginkiss as the administrative contact. Clearly we had a difficult time figuring out who was responsible for that website based on the whois data.

In a similar instance, there was a case that didn't have as interesting a false entry, but there was a case we had where the address was Herehere, California. We have also found websites registered to Mickey Mouse, to God, to Hacker, Bill Clinton, FBI, you name it. And the inaccurate information is really a serious problem.

The second major problem that we have with the database is the searchability. We can go back a few years ago, and the .com registry, there was only Verisign, or Network Solutions at the time, that was the sole registrar for .coms. And at that time, when it was all centralized, it was much easier to conduct our investigations.

With the advent of competition amongst

registrars, what we have found is we are having a more difficult time in finding out additional information about websites through usage of the whois database. And principally, up until about a year ago, you can go to the Verisign whois database and you could search on multiple fields.

So, you could search under the name of a registrant and you could find out a listing of several -- there was a time-out on it, but substantially all the websites registered to a given person. Which helped us considerably, because what we find in case after case after case is the perpetrators of a fraud often have multiple websites that they use, and if we can't search across multiple fields, such as an address field or a name field for the registrant, we are only going to see one part of a fraud and we are going to miss all of the other tentacles that emanate from it.

MS. MITHAL: Thanks, Dan. Dan, you mentioned two issues, the first is I guess accuracy and the second is searchability and I thought we could use that as a framework in our discussions for this issue.

So, first about accuracy, I know that the OECD has done some work on this topic and I thought I would ask Michael Donohue to describe some of that for us.

MR. DONOHUE: Thank you, Maneesha.

I would like to be able to talk about the kind of work that we have done at the OECD, but it's really work worth doing and we haven't quite finished it, so I can't say where exactly it will end up, but it's been going on for some time. It involves primarily the consumer policy committee at the moment, but tax revenue experts as well have been looking at the issue, and even going further back, some of the Telecom policy folks. We also have privacy and security experts, so we're trying to all talk to each other to come up with some common themes.

In the consumer area, we're looking at it from the perspective, two perspectives, really, one is with a view towards increasing transparency integrity of domain names for consumers themselves, and this comes out of the OECD guidelines, the 1999 guidelines on consumer protection in the electronic commerce, which called for businesses to identify themselves for the benefit of building consumer trust.

The other primary and really in a sense more critical uses for that are consumer protection law enforcement, working so that Dan and his counterparts around the OECD countries can do a good job protecting consumers by identifying websites that are committing fraud.

And, again, this is work that flows out of the guidelines to some degree, again, one principle calls for businesses to identify themselves, not just for consumers, but also for law enforcement. The focus here is on commercial usage of the Internet, of course.

MS. MITHAL: I'm just curious, does anybody have any statistics on accuracy of whois data, anything that people know about the ICANN complaint form where people can file complaints about accuracy?

Mike?

MR. PALAGE: I was talking to Dan Halloran, and I believe that the Internet GOTNET website has been up now for about six months, I believe, and I believe that they have received approximately 4,500 complaints to date. Now that would just be in the .com, .organize and .net space. The most interesting statistic that Dan has relayed to me has been in connection with most of the complaints are related to spam.

So, the majority of the complaints, people submitting, if they do state a reason why they believe it's inaccurate, has generally been in connection with spam that they've received.

MS. CADE: If I can just add to that.

MS. MITHAL: Would you identify yourself.

MS. CADE: I'm Marilyn Cade with AT&T and I am

the cochair of the Whois Task Force. Just to follow on what Michael said, they actually today have received over 6,000 complaints. So, the number of complaints and the usage of the centralized form is really working quite well, and there's been apparently significant increase using the complaints as people have become aware of the availability of the Internet form.

MS. MITHAL: Dan?

MR. SALSBURG: Sure. We recently engaged in a search with fellow law enforcement of based on spam that had remove me or unsubscribe lines, and then we went to the whois databases and we got the email addresses for the websites and sent out emails asking to be unsubscribed or removed, and I believe 21 percent of those email addresses that appeared in the whois database were false, they were inaccurate.

So, I imagine it's impossible to extrapolate from that that 21 percent of all entries in the whois database are inaccurate, but certainly in websites that have claims that appear to be deceptive, inaccuracy is a serious problem, and those are the types of websites that we really care about.

MS. MITHAL: Marilyn, I know you mentioned you cochair the Whois Task Force and I was wondering if you could summarize some of the recommendations of that task

force with respect to accuracy of whois data.

MS. CADE: Sure. I would love to do that, particularly since some of the other panelists here either helped to launch the task force, Paul Kane, or are on it now, Phillip Grabansee, we've all worked very hard to try to reach a set of recommendations. When the task force began with a survey and some of the findings of the survey, I will just very quickly mention, because I think they may be of relevance to this.

We did ask people in the survey how they use the whois database, and the uses of the database are the kinds of things that one would expect, people use them in order to find out who is behind or operating a website. They use it in order to solve technical problems, they use it in order to find out whether or not a domain name is available to register, and of course law enforcement uses it. Sort of the typical things that one expects.

But the things that might be kind of interesting. We asked the question of what best describes your attitude toward access to the data in the whois service, and the findings are as follows: And, again, this is a survey that was done more than a year ago, we don't consider it statistically valid, but think of it as a snapshot of what people have responded from

their own personal views.

Forty-two percent use whois as effective identification of who is behind a specific domain for consumer protection or intellectual property protection purposes. Another 27 percent think that it should be available and accessible because it supports the resolution of technical problems on the Internet. And another important point that is important to make is that 20 percent of the respondents did identify an interest in protecting the privacy of individual domain named holders.

So, when people responded to how they used it and what they thought about access, the primary responses were in those three areas. We found that 42 percent of the respondents said they had been harmed or inconvenienced, and that of that, close to 40 percent said that the data of the whois records they relied on were inaccurate, incomplete or out of date. So, roughly 40 percent said that the whois records that they're accessing, not all just because of fraud, were inaccurate or out of date.

The task force has recommended an initial short set of recommendations. Data is not always inaccurate on purpose. We tend to think as law enforcement or as companies who are dealing with enforcement

responsibilities, which we may have in dealing with fraud, we're mostly looking at the data that is someone who may have purposely put in wrong data, but a lot of the data is aged, and so you can't be contacted because your contact information is just too old, it's gone old.

So, one of the recommendations is that once a year, the registrars contact the registrant, present their registration information details to them, and ask them to correct it. And then it is the responsibility of the registrant to do that.

The other recommendation that we made in the area of accuracy is that we provide that I can provide a what we would call a safe harbor. If someone has lost their name, because of providing inaccurate data, that they would go into a redemption grace period of 30 days, and if during that period they presented correct contact information, they would be able to recover the name. It's out of the zone, but they haven't lost it.

The second area of recommendations address the use of bulk access of the whois data, and the task force broadly, and supported by the community, expressed strong concern about marketing uses of whois data. The survey itself expressed strong concern about marketing uses of whois data. Think of it as using the data for a purpose other than that for which it is collected. I

suspect that's a phrase that rings to some of my colleagues's ears, and that was strongly supported by the task force.

So, our first recommendation was to limit all marketing uses of bulk access to the data. Those are the primary consensus policy recommendations. We've made other recommendations that I can maintain the centralized report process for reporting, other things of that nature.

MS. MITHAL: Well, why don't we just focus on the accuracy part of the report and I want to throw open the floor and see if anybody has anything to add or if anybody has any concerns about the task force report.

Ruchika Agrawal?

MS. AGRAWAL: Part of the Whois Task Force's report is to report accuracy, and to me that's like putting the cart before the horse, because surveys have consistently showed that one of the reasons users provide inaccurate information is because there are no privacy safeguards in place.

So, one way to improve accuracy within the question that you've posed, Maneesha, I think is to provide and implement privacy standards.

MS. MITHAL: I saw Phillip first and then

Henning and then Kathryn.

MR. GRABANSEE: A concern with the report, which was participated by myself on the task force, but just a point that I would like to add from a registrar point of view, just something, I don't have a solution to that problem, but just something to keep in mind. It's an economic problem for the registrars, you know, they are operating in an environment with selling domain names with very small margins, and the more burden you put on the registrars, checking the accuracy of whois information, which we all want to be accurate, of course, but it makes it more difficult for the registrars who are already operating in such a difficult economic environment, and it might lead, you know, I'm not sure, but it might lead to a point where we have only, you know, very few registrars who can survive in that environment, and that's something that was certainly not desired when the whole Internet and the whole domain market was demonopolized.

So, I just want everyone to keep in mind that the more burden you take to the registrars, which of course is necessary, because they have to participate, but it has strong economic implications, especially for the smaller and medium-sized registrars and will change the market as we see it right now.

MS. MITHAL: Actually, just before we go to the next comment, I think those two comments provide a good framework for discussion, and I would urge other people to comment on those two comments. Ruchika raised the concern of privacy concerns and putting the cart before the horse and that the privacy concern should be addressed first and then Phillip raised the point about costs imposed on registrars. So, in particular, I would like to hear from people about those two points and what they think of those.

MR. GROTE: My name is Henning Grote, I am with Deutsche Telecom of Germany. Just adding to Marilyn's data from the whois report, we found that due to the fact that most of our DNS customers, our registrar customers, are business users, I would say the aging of the data is about relevant for 20 to 30 percent of the data of the whois per year. This is the kind of rate that gives you an approximate idea of the aging of the data.

The other thing, adding to that what Phillip just pointed out, indeed, it's a big problem to have the costs within a framework that's somehow -- makes it somehow possible to handle in the economic model. But on the other hand, on another technical field, we just started the ENUM trial in Germany, the electronic number

mapping trial where the telephone numbering system is mapped on the -- on a DNS basis.

So, within this trial, for example, we have installed the -- as mandatory -- the policy to validate and verify the registrant. Validate the number that is sent in that should be transferred onto the email name, and verify the registrant, the person, the individual who is seeking after having this number registered.

So, we have now the challenge to put those two worlds together, because one thing is sure, when ENUM indeed goes into reality, and indeed becomes a stand-out technology, we do have to handle this issue of verification and validation of data, at least in Germany as opposed to in most other countries using ENUM, there will be a similar policy.

On the other hand, the issue of costs and the very small margin product DNS. So, this is quite a challenge.

MS. MITHAL: Actually, let me just ask a follow-up question to both Henning and Phillip. You both mentioned the cost issues. Do you have concerns about the costs that the specific recommendations of the Whois Task Force report would impose on registrars?

MR. GRABANSEE: It will certainly be a concern and problem for the -- it will certainly raise some

problems for the registrars. I mean, if you believe in a free market model, you can always argue easily, okay, finally the market has to show that the prices for domain names, I mean the prices registrars take for domain names, they are not regulated.

So, I mean, registrars theoretically are always free, if they can make it or produce it or cannot show a business model to increase the prices, but this will take a long time and this whole procedure will probably put a lot of smaller registrars out of business. And the question is if that is desired, or the other question, you can say that free market interest is just like it is, but I don't have a clear answer to that question. I just see the problem.

MR. GROTE: Just to follow up on that. The question I'm just asking myself is whether the small margin, very low quality product DNS, in some cases, will have a future under these circumstances. The question might be whether other business models should arise, or might arise. Well, I don't have an answer to Phillip's concerns, neither do I have an answer to my own concerns, when it comes to elaborating on a new business model.

I don't know a lot about that, but one thing is for sure, when the -- let's say the quality aspects of

the DNS services, like a curacy, and let's say like a data handling where the customers can rely on, when these are aspects that count, that also means that the -- that our customers have to be educated.

That's on our side. And that's quite an issue. It still has lots of costs, but I would like also to ask the question when we don't do that, how might the market go, and into what direction? Would it go totally down because of the total distrust on the consumer side? I don't know. Just a question. Just a thought.

MS. MITHAL: Okay, Kathryn?

MS. KLEIMAN: I wanted to shed a little light on the privacy issue. And just for whoever hasn't used the whois database, it's a globally available database. When you go to it and you put in information, you get it with the click of a button. For those of us who register domain names for our personal hobbies, to express personal concerns that we have, say, racism or antisemitism, to criticize large corporations for adopting intellectual property policies that we think are too broad, or for political speech, such as human rights or corruption in countries, we don't want our telephone numbers and home addresses available at the click of a button.

The first question that we were asked in

preparation for the panel was how can domain registrars and registries improve the accuracy of whois data and the generic top level domains? There's one easy answer, and that's called tiered access, effectively create the option of an unlisted telephone number or home address.

I come from a technical organization, the Association for Computing Machinery, we've been around since 1947, many of our members were original Internet pioneers. When you go back to them and you ask them what the purpose of the whois data was, they said it was for technical contact. It's to reach someone if your website was sending out, you know, unheard of amounts of crap on the 'net and you needed to shut it down. It wasn't for the purpose which it's increasingly being used for, which is content policing.

So, of course law enforcement needs to reach people, as do others who are suing based on content, but the whois database as it exists is inaccurate because people are trying to protect themselves. Very much in the way, frankly, that the Federal Trade Commission has advised people to do in their consumer identity theft publications, where they say, don't give out personal information on the 'net. That's very good advice. Don't give it out.

So, my best recommendation as we go into this

is, let's draw a very clear distinction, and it hasn't been drawn, in the Whois Task Force report, let's draw a very clear distinction between commercial use of domain names and noncommercial use of domain names.

The second thing I would raise as domain registrars pose the issues of cost is the issue of liability. This is not my organization, but it has been xeroxed and distributed, the Electronic Privacy Information Organization, bullet point number two, yesterday, "The New Hampshire Supreme Court has held that information brokers and private investigators can be liable for the harms caused by selling personal information. In that case, a young woman was murdered by a stalker who obtained her personal information from information brokers and private investigators."

To the registrars, I would say, we are your subscribers. You know, there are people out there, there are disgruntled spouses, there are stalkers, there are governments who want to criticize people for taking democratic, pro-democratic positions, protect your subscribers. Let's figure out a balance, but the single best answer to protecting accuracy, to getting accuracy to whois is giving people the right to create an opt-out where the information is there, it's available to law enforcement and others under the appropriate

circumstances, but not to the whole world all at once.

MS. MITHAL: Before we move further, let me just talk about some of the scope of the discussion we're having here. I think the scope of this workshop is about cooperation between law enforcement and domain registrars and registries in combatting fraud, and I think the points Kathy just made are extremely important points, and I think, you know, those issues definitely need to be discussed further, but I'm wondering for the purposes of this discussion, if we could simply talk about whois data for commercial registrations, the types of investigations that we do generally involve commercial targets.

So, if we just limit it to that for the purposes of this discussion, as people are talking further, I just ask you to do that.

So, Paul and then I saw Willie, and then Dan.

MR. KANE: Thank you, Maneesha.

My name is Paul Kane, ICB from the UK. We are a software house, and we've built a number of systems for quite a few registrars. Just to bring this to perspective, there are 160 ICANN accredited registrars, of which 118, I believe, are currently active. I think it's fair to say that every registrar that is active really would like to provide to the community accurate

information. They don't go out purposely to allow Donald Duck, as the gentleman referred to.

One of the things, I think registrars will be very concerned about, is where the duty of care to check the accuracy actually rests. And that, as Kathy was implying, has costs, and there are some significant issues. And obviously at what point is the data accurate?

At the time of registration, the applicant may have submitted accurate information, and then the day after registration, the person may have moved, there could be a change in circumstance. So, if one delineates between commercial registration and living, breathing individuals, who may require a degree of privacy, because it seems the privacy issue is the one of concern, and in fact the lady at the end there mentioned it, I think it's fair to say within the ICANN accreditation agreement, that registrars sign in order to be able to register in the gTLD lease space, there is already provision for registrants to use the contact information of a third party, where they feel that personal freedom, personal liberties may be infringed.

And so, the mechanism already has that in place. So, the registrar can accurately record the information of a third party. Now, there may be a cost associated

with the provision of accurate information of a third party, but obviously that is the choice of the registrant in exercising that right, if they wish to do so.

We have the pleasure of having Jonathan Bamford here from the UK Information Commissioner's Office, and obviously being from the UK, one of the things is explicit consent, one has to give consent to information being publicly disclosed. And similarly, provided that information, the registrant at the time of registration is aware the information will be publicly disclosed, I think it's fair to say that the registrars will be covered, provided it's made very clear to the registrant at the time of registration it will be available on the Worldwide Web.

And then Henning raised a pretty good point about ENUM. My company, Nominet, are actually involved in the UK in the trial, we're going to be running the tier one where the .44 is going to reside. And one of the big costs that the domain has in the ENUM is not register the domain, it's matching a particular telephone number with a subscriber with an entry.

And so, in the domain name market, which is global by its very nature, one has to be very careful insofar as the duty to supply the registration rests on

the registrant, not any other party. In the case of ENUM, it is the person requiring a number that will need to come with their telephone bill that identifies them, the address, and the phone number. There will be a duty on the registrant. Similarly, within current contracts, I think it's fair to say that registrants place that duty on -- sorry, registrars place the duty on their registrants to provide accurate information.

And the whois report is really trying to make sure that the information that is held on the central database is accurate, subject to these conditions. It's in the registrars' interest to make sure they're accurate, because they want to be able to contact their customers. As I say, there is already provisions to protect living, breathing people.

Another angle, just to complicate matters, is in Austria, the rules are such that companies, corporate entities, not living, breathing individuals, corporate entities can similarly claim a degree of protection under data protection. So, it's very difficult to draw a line because commercial entities and living, breathing people. But it's not in the registrars' interest to gather up bogus information.

MS. MITHAL: And just a follow-up question. You mentioned that individuals have a protection that they

can register through a third party. If I'm a company that's selling, you know, fraudulent goods to consumers, could I hide behind that as well?

MR. KANE: The duty, again, is to the registrant. There is a relationship, a legal relationship between the third party agent and the registrant. Assuming because the third party agent would not want to be liable for any of its customers. So, from a law enforcement perspective, it is quick and easy to identify the third party, and having done so, they can get a direct relationship to the registrant.

So, it's all there, it just needs to be applied.

MS. MITHAL: Willie?

MR. BLACK: Thanks. I'm Willie Black, chairman of Nominet UK who manages about four million domains in the .UK top level.

I'll try and be quite brief. I think I'm complementing what other people say. It's important to us to know who the other party to our contract of registration is. After all, it is a contract, and you don't want to contract with somebody that you can't chase out for money. But it's very human intensive, what we're talking about here.

In the UK, we have money laundering things, and if you try and open a bank account, you've got to send

in a copy of a utility statement or a copy of your passport or something like that, and this has to be verified. It's very human intensive. And in Nominet, we've just realized that we cannot keep affording to do too much intensive human checking. Which is a pity really, but if it has to be done, of course we will be happy to try and do it as sufficiently as we can.

But even in spite of the cost, you see, good people do want their data to be correct, and I'm here talking about trading, not the personal one, and we do give an opt-out in .UK to people to register an agent if they want to hide, because of personal threats.

But talking about businesses, good people do usually want their database to be correct, and so they -- the whois is useful for them to check that it's correct, but the lot of them are very lazy and they move premises and they just forget to change things.

So, again, a renewal period of two years that we do is actually quite a good time to be catching up with people. Although you might just find that you send the invoice out and you never get any money back. And then there's a lot of problems.

But the real point of my intervention is, is the crooks actually are quite clever. They don't go around with a bag marked swag, you know, or a striped jumper,

and they're not going to write Mickey Mouse down when they're perpetrating 100 million pounds in fraud, huh? They're going to put a perfectly reasonable business name that you just can't trace very easily.

And of course before there's an issue arises, nobody can tell that it's wrong, without you going and checking that such and such a street number at such and such a place actually exists is going to look perfectly reasonable. And so you can only react once it's been discovered. And of course the registries would be very happy to try and chase down the issue at that point and see if there's any forensic evidence that it would be, you know, that it was some real business or a fraudulent business.

One thing that we do suffer from in the domain name business is that we are private entities. We don't have the power to fine. If you declare the wrong thing on your vehicle license in the UK, I think it's a thousand pounds, you can be fined. Because there are statutory bodies and they can fine you for making a misdeclaration. I don't know how often it happens in the UK when people forget to change their address when they move house, and they don't reregister their car, but we cannot fine. And that is an issue. All we can do is really cut people off and they lose the domain

name, and if they're really crooks, they just go and relaunch with a different domain name.

So, that was just some thoughts that came from the other speakers.

MS. MITHAL: Thanks. Other remaining people who have tents up, I would like to ask people to focus on the question of if, say, law enforcement said, look, you know, we want to improve the accuracy of the whois database, as registrars and registries, you know, what can you do to help us? Can you implement the recommendations in the Whois Task Force report, is there anything you can do above and beyond that to ensure the accuracy of data. I would like people to address that point if they could.

So, let's have Dan and then Mike and then is that Wayne?

MR. MacLAURIN: Sure.

MS. MITHAL: Wayne and then Jonathan. Why don't we stop at Wayne and then we can go forward.

MR. SALSBURG: I think Willie raised a very good point, and that's that the registrars do have an economic incentive to ensure the accuracy of the data. Otherwise, how are you going to know who to send the renewal to, how are you going to know who to bill again? And the question is that how do you ensure that this

accurate information that you may have in internal databases, because you have that incentive, getting in the external database that is viewable by others. And do you collect this and keep it in essentially two sets of books, or do you cross check it and try to ensure based on the information you're collecting for billing purposes that your whois data is accurate?

And, in addition, there are proactive steps that it sounds like some of you already take in trying to ensure that the whois data isn't just garbage. Do any of you also do things like ensuring that zip codes match addresses, those kind of basic things that at the very least it will cure the honest person making an error. It may not stop the actual person engaged in fraud, but still, the person engaged in fraud from your own economic incentive, they're not the ones that you want to ensure that you can renew their registration, it's the people who mistakenly missed a digit.

So, those are two questions for you. And I guess I'll stop there.

MS. MITHAL: Okay, Mike?

MR. PALAGE: Yeah, just a couple of quick points here. Within the past week, I've talked to three registrars that have voluntarily began to implement CVV2 and address verification, not because of what the Whois

Task Force recommended, not because law enforcement had asked, but because of a business decision, they were hit with tens of thousands of dollars in credit card chargebacks.

So, as I said, I think Phillip here hit on a good point, registrars, most registrars are as Paul said, 160 registrars, each with its own unique business model, but most of them are legitimate businesses trying to provide a service and they are trying to have the valid data to get renewals and stuff like that. And some of the steps that they are taking to identify inaccurate data I view as a positive step in the right direction.

One of the things I think most registrars are at times concerned with are unfunded mandates by third parties, without a proper cost benefit analysis. And, again, just an example to sort of follow up on what Willie had mentioned earlier, good people wanting to have accurate data, it took me last year and a half ago, it took me three months of faxes and emails to get my particular registrar to update the data. The data wasn't updated, and my name was deleted -- well, it was expired, I had -- it was quite difficult. And I consider myself a good person who has accurate data.

And the change there was because of an email

change, which as Marilyn can say from her company, who has had different carriers, there's been a lot of users that have had numerous email changes. So, again, when Willie was saying good people wanting to have accurate data is true.

The one other thing about bad people being very smart, and I think I had raised this with you was, I recently was involved in working with a large corporation that what happened was a certain environmental group had an issue with a particular chemical company, and they registered a protest site in the name of the son of the president of the company. They had his address, they had everything right. So, again, you know, this was some place where the smart people or the bad people are quite smart and sometimes they could actually be quite ironic and devious all wrapped up at the same time.

So, again, when you look at this, registrars, I think, overall, want to have accurate data because it's a business decision for them, they are just at times concerned with unfunded mandate without the proper cost benefit analysis. So --

MS. MITHAL: Wayne?

MR. MacLAURIN: To give you an idea of what this actually costs us. The ICANN, Internet.Net mandate to

check whois, probably take us two to three hours per incident to actually track down and verify from the time we get the initial complaint and closing it on the Internet. So, that's a pretty high cost for us to assume, right? And we're happy to do it, because, as you said, we want the information correct.

But it's not easy for us to verify that info. Either manually or automated. Yes, it would be nice if we checked zip codes, but that's easy, because the U.S. has zip codes and a fairly well published database. It's a little bit harder in Botswana, and much, much harder in parts of the old Soviet union, where the naming conventions are all over the place.

Even in the States, we can get a perfectly good address in New York, and a phone number from Jersey. Is that accurate or not? The fact is that the guy has a cell phone that's been issued from New Jersey and it works quite happily. So, this is not an easy thing for us to fix or track or find. And I think you need to be aware of that. There is no easy fix.

I know somebody who spent a great deal of time and built a very big database trying to figure this out, and it's on the order of gigs of data that they have to mine to try to make a guess at a match. That's a nontrivial exercise.

MS. MITHAL: Let me just follow up with a question. You mentioned the cost for following up on ICANN complaints that they refer. From a cost perspective, are there any kind of up-front verification methods that could save those post hoc costs down the road?

MR. MacLAURIN: Well, certainly there are a few ways to validate some of the information, right, and there are some third party options you can do. There's certainly some stuff you could do internally. One we would love to do is to have the credit card companies actually provide us a uniform method of checking information. Visa is quite happy in the States to verify card, address and zip code, I believe, that doesn't exist anywhere else. Canada, it's card number and expiration date.

So, there's no way for us to check to see whether or not it's a fraudulent charge, even the fact that it's the right information, the right card number, we can't validate that. And so it -- there are some solutions, but none that are particularly broad.

MS. MITHAL: I want to wrap up this discussion on accuracy. So, the people who have tents are Kathy, Ruchika, Chris and Jonathan. So, we can go in that order.

MS. KLEIMAN: I know, Maneesha, that you have drawn the distinction between commercial and noncommercial, but the registrars at the table represent both and my concern is always that the policies we adopt for one should be clear as to who they apply to, particularly if the intent is only to make them apply to commercial, what is it going to do for those who are using domain names for noncommercial.

Paul Kane has mentioned a solution that they've come up with in the UK that doesn't really work internationally, that if you want to protect -- that domain name holders using their domain names for noncommercial purposes have to go to a third party in order to have any privacy. That third party will have the liability probably for whatever speech they put on.

So, that's the last place that you want to go if you're talking about human rights abuses, torture, corruption, no third party is probably going to want to take on the liability of hosting, or being the name of representing that speech or being held out to represent that speech.

I mean, people use the Internet to communicate their own speech, they want to communicate directly. So, accuracy and privacy go hand in hand really to me and the idea of creating tiered access, and I was

wondering if anyone -- can I pose a question, because there are technologies out there that are being developed, including one by the IATF called CRISP, I understand, that would allow kind of a tiered access and allow people to obtain and opt out opt in and opt out. So, the data could be accurate, but just not all globally available at the same time.

MS. MITHAL: Does anybody want to respond to that? People who have tents up. If you would like to, you can. If not, that's okay.

MS. AGRAWAL: I was going to -- that's a good question to pursue. I was going to ask two different questions. I think the FTC should consider how the global public sensibility of whois information actually contributes to fraud, to identity theft, to spam, and to some of the issues that were mentioned before. I think that's an important study, and the FTC should see how that impacts them from that sense.

The second question I want to read is if we were to draw an analogy with the abstaining subscriber information, law enforcement has to get a subpoena or court order or search warrant to get subscriber information. Why not apply that to domain name registrants?

MS. MITHAL: Chris and John?

MR. DISSPAIN: Yeah, Chris Disspain from Australia. I just wanted to -- the topic for discussion is accuracy of the data, as I understand it at the moment, not necessarily its availability, just the accuracy. In Australia, we do much the same as the task force has recommended, in that we insist that our registrars contact registrants to check their data on a relatively regular basis. And in any event, presumably, even in the GTLD space, registrars contact registrants when their domain name is up for renewal.

If you take Willie's point that the crooks are going to lie anyway, and the good people want their data to be accurate, is it not sufficient to have a situation where if when you come to renew your name, you're effectively warranting that your data is accurate, and the registrars are simply checking to make sure that they can contact you. If you can't -- if you can't contact, you can't renew. If you can contact, then surely that's sufficient. I don't see that there's actually -- I think that solves the accuracy problem.

MR. BLACK: The crooks don't care.

MR. DISSPAIN: They don't care, exactly.

MR. BLACK: They'll make a warrant. I mean, if they're going to steal money from people, they don't mind warranting to you that it's accurate.

MR. DISSPAIN: The question is if we're talking about accuracy of data, then as you say, Willie, good people want their data to be accurate. People do not walk down the street every day thinking of their domain name, although it may sound, but they do think about it when it's time to renew it, and at that point, you can check the data. If what we're talking about here is actually accuracy of data of crooks, that's actually something slightly different, and that's much more complicated to get to the bottom of.

MS. MITHAL: Jonathan?

MR. BAMFORD: Just to deal with a couple of points as a co-op, and I know you don't want to deal with a whole raft of privacy issues, but I'm not quite certain that it's so easy to side step what falls into data protection areas and what does not. Because I get the impression that somebody operating on a domestic basis is covered by a data protection and somebody who operates on a commercial basis isn't. This isn't actually true. If you're a living individual and you're operating in a business context, data protection law still applies to you.

So, anybody who operates as a data protection consultant, Jonathan Bamford, data protection consultant, there will be personal data about me, even

though I'm operating in a business context. So, it's hard to park the sort of privacy issues to one side there.

And the second point I would just make is that in those instances where data protection law does apply, and then one of the requirements is that personal information is accurate and kept up to date. And so it's not just a question of people being virtuous in terms of keeping information accurate, there is actually a legal requirement when it's personal data to keep it accurate and up to date.

Reasonable measures to do that and extracts may be some of the things that have been suggested there in terms of updating it at a reasonable frequency, and asking people may well be the reasonable measures, given the nature of the information.

MS. MITHAL: Okay. I'll give Dan the last word on the subject.

MR. SALSBURG: Thank you. One of the themes I've heard from Willie and from others is that if the data that crooks submit is going to be inaccurate anyway, why even have this conversation, why do we care? I think that there are two issues there. One is that vastly overestimates the intelligence of the majority of crooks. We have been highly successful in the cases

that we bring, using whois data as the building blocks for our cases. That's the first point.

And the second one is that even in those instances where we have found inaccurate data, when we have been able to search along other fields, we have been able to find patterns that have been able to tie numerous websites together as being -- pointing to the same culprit. For instance, same address, where there's a same contact name, or even if it's a same false registrant. The fact that there was a same registrant and same false information has enabled us to put cases together pretty quickly.

MR. DISSPAIN: It's about access to the data, not the accuracy of it.

MR. SALSBURG: Well, it's both, clearly.

MS. MITHAL: Okay, thanks, Dan.

Actually we started getting into the CCTLDs and what some of the policies are in the CCTLDs. So, I thought we could start by just asking Michael Donohue, I know the OECD is working on a report assessing some of the policies of the CCTLD. So, Michael, can you summarize or tell us anything about that report?

MR. DONOHUE: Again, not as much as I would like, hopefully the report will be finalized in the next few weeks and will be available on the website for

anybody who is interested.

UNIDENTIFIED SPEAKER: Excuse me, could you speak into the mic, please.

MR. DONOHUE: Sorry about that. Is that better?

It's just a study of CCTLDs, the administration of CCTLDs, and it's limited to the OECD countries, so it's far from a survey of the whole world, but it does show that there is an increasing -- registrations in CCTLDs are growing at a faster rate than they are in the GTLDs. They have doubled between July of 2000 and July of 2002.

The rules and policies used to administer CCTLDs vary quite considerably within the OECD. Although most all of them have a whois function, the information that's available in the whois function varies quite considerably, particularly with respect to the contact information that we've primarily been focused on, I think, today.

Around 70 percent of CCTLD domain names in OECD make the contact details available via whois according to our preliminary information. So, there will be a lot more in this paper, but I'm sorry, I don't have it yet for you.

MS. MITHAL: Willie or Chris, do you want to add anything to that specifically about .AU and .UK?

MR. DISSPAIN: Can I go first, Willie?

MR. BLACK: Yes, thank you.

MR. DISSPAIN: It may just help to give you a very brief outline of what we do in Australia. We introduced a new regime on the 1st of July last year and that, in fact, led to a significant reduction of the amount of data we make available in the whois. Our data is relatively accurate on the basis that there are significant policy hoops that people have to jump through in Australia in order to get a domain name.

.AU is only used for companies, for example, for people in business and so on, and it has to be a connection between the registrant and the name. So, from an accuracy point of view, because of the fact that we have policy, unlike the GTLD space, which doesn't have any, our data is actually accurate. Most of the data that is inaccurate is inaccurate because, as I said, people don't spend their time thinking about their domain names until it comes time for renewal.

We actually have a redemption period if the registrar tries to get in touch with you and your domain name expires, you've got basically 14 days to renew it before you lose it. You would be amazed at the number of people who don't realize that their domain name is not working for months.

But particularly, the availability of the data is what I wanted to briefly address with respect to Australia, and that is that we now simply say, show the name of the registrar, the name of the registrant, and an email address for the registrant to contact, and the same for the technical contact. We do not provide an address, we do not provide a telephone number, we don't provide any other data. We have that information, but we don't make it public.

Now, what we have, our equivalent of this body is the ACCC, and we have an agreement with the ACCC that they will send us a simple form if they want to find out the information and we will give them the information, to a degree. But we believe that to publish the information so that literally anybody can look it up is a recipe for disaster and has, in fact, been that in Australia where the database has been misused, abused, and people basically just got to the point where they said we're not prepared to put up with it anymore, and there is no circumstance here which I can see Australia going back to a situation where full data is published. It just isn't going to happen.

MS. MITHAL: Okay, thank you.

Willie?

MR. BLACK: Fairly recently, the UK is one of

the older top-level domain country codes. We've probably been talking registration since the late eighties, I guess. And some of the information was fairly crude. And, in fact, up until very recently, we just basically announced to the registrant laws, but listening to other people around the world and in the ICANN framework, and indeed folk who wanted to know a little bit more information than intellectual property consistencies, we decided that we would extend it.

Now, our first point is that we are trying to get away from the old concepts of admin and technical contacts. We believe that the technical contact is associated with the service, and so that's one thing. And the contact, the admin contacts, basically our prime concern is who the registrant is, because that's who we've got the contract with. And that can be a company, it could be a partnership, it can be a sole trader. There are many types of legal entities that can trade. Or not. Or indeed contract, I think that's the word I want to say.

So, we decided that we would publish the name of the registrant and an address. We declined to publish telephone numbers, fax numbers, or email addresses for the obvious reasons that we don't want people being phoned up and we don't want people being spammed with

their email addresses. We do have such information for the registrant, but we keep that in our private database. So, we have a database of all our registrants with this extended information and we simply feed the whois with the name of the registrant, and an address.

Now, in order to do this, we went through our policy-making process in the UK, we have a policy making board that contains both our registration agents, we've got about 3,000 of them who are almost equivalent to registrars, but there is a fine distinction, and they elect certain people. We also have a consumers person, we have a government department of trade and industry person. We've got another eight stakeholder groups involved in the policy board.

And the policy board discussed this, and we actually went to wide consultation with the public, and said, guys, we're going to public addresses, and of course we had quite a few people saying, no, my teenage daughter's address isn't going to be put up there. And the stuff that Kathy was quite reasonably mentioning. And so we did give them an opt-out, and the opt-out is that they can use their agent, which is basically the equivalent of the registrar, but only if it's a person and they're not trading.

You see, in Europe we have another directive

called the distant selling directive, and that compels somebody who is trading over the net to actually reveal where they're trading from. And so even a sole trader who is trading must declare where their address is on their website, so therefore there is no down side to them declaring it and us having it available in the whois.

So, with all that, we made the change and we're gradually rolling this out so that there will be an address there.

With respect to revealing the extra information, our data protection contractual terms allow us to give it away to the authorities that would be making an investigation, how formal that needs to be may depend on where the request is coming from, because obviously we don't want to be giving away the information to somebody pretending to be doing an investigation who really isn't.

And so there is an issue there, I'm sure we'll get around to things like that later. But just before I stop, I want to point out that I'm also chairman of CENTA, which has got 30-odd other CCTLDs there, and I notice this whole meeting has been rather Anglo-Saxon oriented, if you don't mind me saying, we've got some German colleagues here, but for the most part, it's

been, if you like, the common law countries, Australia, Canada, the U.S., the UK. And, in fact, within CENTA, we have, of course, other EU members, but we've also got the former Eastern Block, you know, the Polands, the new Europe, that's right. To make a topical diversion, thanks, Chris.

And, actually, we have even a member from Iran. Now, you've got surreal countries and you've also got many other countries in the whole panoply of the CCTLD world that don't actually quite have the same contractual view of life, and that don't have quite the same views of privacy, and some of the issues that western democracies may value.

So, we've got to remember that even within the Channel Islands, they have quite a distinct kind of thing that they're near France but yet they're part of the British Isles, but they're not part of the United Kingdom and they're not part of the EU, but they copy a lot of our internal stuff from both the EU and they've got some of their own.

So, do remember that although we're talking here basically about common law countries and the general contractual framework that we live in, the world of CCTLDs is quite diverse. So, that was just a little point I thought I better make.

MS. MITHAL: Thank you, Willie.

I would also like to ask if Wayne or Henning, you have any comments to add about .DE or .CA.

MR. MacLAURIN: Sure, the CA world has actually sort of gone back and forth. Back in the good old days, pre-competition, pre-anything else, it was actually pretty hard to get a CA domain. First of all, you had to figure out who was selling them, which was a nontrivial task. And then they had the rules where if you were a corporation, you could have -- if you were a Canadian corporation, you could have .CA; if you were a provincial corporation, you got sort of a geographical, just .ON.CA; you know, Ottawa.ON.CA, if you happened to be personal.

So, all this was a little bit easier, because if you were a Canadian corporation, you showed up in the Canadian corporation database and it was kind of easy to validate that that's who you were.

They've gone kind of the other direction since then and although they still require you to define what you are, if you're a Canadian corporation or anything else, the domain itself is relatively open. So, we can still validate some of the information in terms of if somebody claims to be a Canadian corporation, we can validate that, but it still leaves it wide open if you

came to an individual, for example.

Our CERA, who is our overseeing body, does check the information and they do submit requests for validation on a regular basis as part of their ongoing registration process. Fairly like Australia does as well.

MS. MITHAL: And what fields of data are available?

MR. MacLAURIN: It's a lot like whois, although it is a fat whois, in terms of it's controlled by CERA. They do show the registrant, the new contact and old contact information, address phone numbers and email.

MS. MITHAL: Thank you.

Henning?

MR. GROTE: In the ENUM space, it's a bit different, it's quite -- it's been changing now. The data that is available is restricted, not when it comes to access, but to the number of different date fields that are shown. And right now I just received the actual -- I don't know the exact English expression, but the -- when it comes to privacy, the data protection commissioner of the federal state where the DE Nic, the top authority for the DE name space is situated, is located. This chief commissioner just issued his report about a privacy data protection in the DE name space,

and there the opt-in is asked for.

So, that means for living, breathing individuals, I like that expression for private persons, there should be provisions for an opt-in in the whois database. That means if they don't use the opt-in option, there won't be any further information than just the name of the registrant, as I interpret it. But we have to go deeper into that issue, it's not implemented yet. It's still on.

I think hearing these comments from some of the CCTLD representatives, it seems clear that the policies vary pretty widely among CCTLDs, and I know, Marilyn, that the Whois Task Force was looking into this uniformity issue, and I'm wondering if you could just tell us what happened on that.

MS. CADE: In relation to -- let me -- one of the questions we ask, several questions we asked had to do with uniformity and consistency of data elements, and then separately, we asked questions about searchability.

The task force was very much taking the point of view that accuracy can be separated from access, and I think we're hearing some examples of, in fact, where accuracy and access are related to each other, but not necessarily a one-to-one match.

In the consistency of data elements, we will be

putting forward an issues report which is likely to say that uniformity and consistency of data elements needs a sort of wait and see approach before implementation.

Certainly there's standards work that is going on that needs to -- would call it ripen further, and anybody in this room who has been involved in standards knows that there's the development of the standards and then there's the publication of the standards, and then, oh, there's the adoption stage of the standard. So, just because we're making progress on getting standards matured, I would say in the development process, we've still got a ways to go.

So, the issues report will recommend that people work more actively within the standards process. In the issues of searchability, the issues report is likely to say that in the implementation of consistency and uniformity of data elements, and in searchability, that there can be increased challenges with possible profiling if there are not protections implemented at the same time.

So, that is sort of on hold. We did -- or will be, I think, recommended to be on hold. We did look at and asked the question of do you expect uniformity and consistency of data elements in CCTLDs and in GTLDs, and there's strong support for uniformity and consistency of

data elements across the GTLDs and also in the CCTLDs.

In our conversation with CCTLDs, I think what we were hearing, and we did talk to some, we talked to Canada, we talked to Mexico, we talked to a couple of others, there are CCTLDs who actively do data checking before they enter data. Most of the CCTLDs, and maybe Paul might want to comment on this, are really looking for effective software applications, and so the feedback we got was we'll be waiting, like everyone else, to see if there's a useful standard, and when the standard is available, then we'll be interested in considering deploying it, but it doesn't seem to be something we would leap into right now until the standard is available.

MS. MITHAL: Thank you, Marilyn.

I'll call on the two of you next, but I just wanted to ask Chris Disspain a follow-up question, and I should mention that Chris came in from Australia last night, he is leaving at 4:00 today to go back to Australia. In fact he has to leave at quarter to 4:00, and so I want to make sure to get in all my questions to him. I think he wins the prize for dedication to this workshop.

MR. DISSPAIN: Actually I didn't come in last night, I did stop in LA. I was forced to stop in LA.

due to snow.

MS. MITHAL: Thank you for coming.

MR. DISSPAIN: My pleasure.

MS. MITHAL: To follow up on something, you said there were not publicly available information in the data fields to the public, and I guess my question is let's say the FTC, for example, were investigating an Australian website that was targeting U.S. consumers that ended in .AU, we didn't see that information in the whois database. Is there any way we could access that information?

MR. DISSPAIN: Well, I guess there's several ways that you could access that information. I imagine that you have some kind of arrangements or consult talking to your equivalent in Australia about all sorts of things, and I have no doubt if you ask them if they would ask us, then they probably would. If you asked us yourself, I don't actually -- it hasn't happened.

I guess the answer would be that -- see, it's complicated by this particular point: If we were investigating -- if the Australian authorities were investigating something in the States that was illegal in Australia but legal in America, how would that pan out for you, and the same way that if we -- if what you were concerned about wasn't actually a problem for us,

I'm thinking, for example, about pornography, as an example.

I mean, we have what our government likes to refer to as content legislation, where most of us refer to as a complete and utter waste of time, but nonetheless, they seem to think it's important. And if we were trying to get hold of some information about U.S. people who were doing things that weren't necessarily illegal here, how would that work, from your point of view?

So, it's a very complicated question to which there is not a simple answer. If we get a request from our authorities, then we will obviously provide that information to them.

MS. MITHAL: I think we're going to follow up on some of these issues a little more after the break, but I just wanted to get Chris' perspective before he had to take off. So, let's have Paul and then Mike and then Ruchika, and then that will be the last word on this issue.

MR. KANE: Thank you, Maneesha.

Just again a few more statistics. There are 244 country code top-level domains, of which 118 have online whois databases of one sort or another. We have learned that various registries, CCTLD registries, publish

various data elements, and we've also just learned, and it's very obvious that the registries have to abide by the law of the country in which the registry is based.

And so, whereas there is no get-out for criminal activity, there is, I think it's fair to say, within all data protection legislation, if law enforcement asked for information and provided the appropriate documentation, then whoever holds the information must provide it to the respective party. But it means in the international context, probably, and I'm guessing, as Chris was referring to, that one had to go to the ACCC and ask them to get the information rather than anyone else.

But the point I really wanted to make was to highlight, as Willie alluded to earlier, the different relationships between CCTLDs, the registrars and the registrants. Willie is able, in the UK, Nominet, the relationship is with the registrant. The registry has a direct contract with the registrant. In GTLDs -- and therefore Nominet, let's say, owns in the broader sense, the data.

In the GTLD space, there's a difference, insofar that the registrar may, in certain circumstances, own the data. And so, and we have an agency relationship where the registrar may be an agent of the registrant,

in some jurisdiction, or the registrar may be an agent of the registry.

So, there are a whole range of different areas. In terms of searchability and having some uniform format, a few years ago I was the European representative of the registrars when in Germany, the Federal Data Protection Office wanted to jump on all German registrars because they considered the provision of bulk whois information, which accords with the registrar/registry agreement, was in violation of German data protection law.

And that would obviously have created a bit of a political situation. And fortunately, we were able to smooth the waters. Subsequently, there are other restrictions in Europe and elsewhere which are trying not to go down a uniform approach, which I find a great shame. It would be great to have a uniform manner, but one of the issues is if this is pushed rather hard, and reference was made to searchability, one of the fears would be that enabling data to pass across national frontiers, in a searchable format, could present significant challenges within the European Union area, within Argentina, within Israel, within Japan, and cause a fragmentation of this thing that we are trying to keep united, the whois.

And so in CCTLD land, where registries must abide by national law, one needs to be very sensitive to the fact that registries' first duty is one accord to national law, but also to try to have this uniform framework. If one tries to have lots of searchability that the gentleman is referring to, yes, it was great in GTLD land, but one needs to be very, very sensitive to the various requirements within CCs, because otherwise people will start shutting down, as Austria -- I'm sorry, Australia has done, and I really want there to be, as I was discussing with you yesterday, the concept of having differential access for different parties brings a whole rash of problems.

One, you have to identify who the owner of the data is, and two, you have to identify if it's an appropriate agency that's making contact. And so if anything, it will frustrate law enforcement, who are actually trying to help and trying to get the bad guys.

MS. MITHAL: Thanks.

Mike?

MR. PALAGE: Actually, that was actually an excellent segue. Going back to what Commissioner Swindle said earlier today about I don't want to hear about the problems, I want to hear about solutions to solving the problems. Following up on what Paul just

said, there's 160 registrars in a number of jurisdictions. It is very difficult for them if they were to receive something from the ACCC from Australia, they would say, who is this.

It really represents an alphabet soup of agencies which makes it rather difficult for registrars, and as Phillip said, there is a lot of small, mid-sized registrars that think this is very complicated. One of the ideas that I would like to throw out, and maybe this is something the FTC could bring up with their GAC representative within ICANN, is that, what is it, about a year and a half ago, ICANN passed board resolution 0192, which dealt with the country names on the ISO 3166 list in the .info space. And what happened there was the ICANN board basically said take these country names and make sure that the appropriate government agency can register it.

Now, that sounds real easy, but one of the things in ICANN is when something sounds easy, actually implementing it becomes quite difficult. And one of the things that I have been working with is a consultant with Afilias who is trying to identify who can speak on behalf of Germany.info.

And, again, to use the example, there were actually two names on the list, Germany and Deutschland.

And the system that was put in place was that if there was a request from a government saying I want this name, what Afilias or what ICANN did was they would contact the GAC representative -- they would contact the GAC secretariat and then ask the secretariat to go to the appropriate government and say, who within your government can speak for this domain name? Who would be eligible to register it?

So, that actually from Afilias' standpoint provided somewhat of a uniform standpoint to make sure that the right person got it.

And I guess this is what Paul was saying, is if maybe the governments were to work to identify who is an appropriate law enforcement agency, because again, you wouldn't want some potential sheriff in Podunk, USA trying to have access to, you know, data. Again, you need to have sort of a tiered access approach.

And I think that's one of the ideas you may want to consider of how to use the GAC in a constructive manner to make it simpler for registrars to work with law enforcement in addressing these situations, while simultaneously going towards what I propose, which is sort of a tiered access to the whois, where you have law enforcement, the intellectual property or business community, and then individual registrants. I think

that that tiered approach is part of what a long-term solution is.

MS. MITHAL: Thanks, Mike, and I think I would really take both of your points about, you know, how to know whether a law enforcement agency is who they say they are, and I would like to kind of save that discussion for after the break.

Ruchika had her tent up and if we could just close the discussion on accuracy and searchability of whois data.

MS. AGRAWAL: Well, I am on the Whois Task Force as a noncommercial constituency representative and I work for the Electronic Privacy Information Center. I am going to put on my techy hat for the moment and I am going to talk about a new protocol that's being discussed by the Internet Engineering Task Force and that's called the EPP, and basically it's going to standardize whois data and it seems to speak to uniformity. I think it seems to me that many of us at this table should probably think about the issues and the questions that's going to raise for many of us, and I'm not sure if Marilyn wants to address the uniformity issues report, if we're talking about the EPP protocol and how that may impact our issues report.

MS. MITHAL: Do you want to respond?

MS. CADE: It's CRISP. We should just clarify the EPP protocol is a registry protocol, and there's a discussion within the IETF Task Force about whether or not to add either extensions or tagging to each of the elements, but CRISP I think is the protocol that we've been talking about the IETF developing, which could lead to uniformity for whois.

Both of those would clearly have -- but again, it comes down to how is it implemented, because you could certainly have a standard which has capability, but not turn certain features on in the implementation. And as we heard in the Whois Task Force, and everybody here who works on the IETF is probably tired of hearing, there's technical standards and then there's all this policy stuff. And the policy stuff seems to always impose into the technical standards.

Again, I think in our report, what you are going to mostly see us say is there are a lot of questions, and they need to be really thought about, because implementation would be done in one way and might lead to the ability to have easier data profiling, and implementation could be done in another way and searchability would be there, but it would not be a feature that was turned on unless it was authorized access.

MS. MITHAL: Thanks, Marilyn.

Okay, well, let me just summarize this discussion, and I just think that I've taken maybe three points out of this, three main points. One is that there are privacy issues, and we need to continue to work together to figure out how to deal with those issues, and so we should have continued dialogue there. I think there's general agreement at the table that law enforcement, bona fide law enforcement, should have access to accurate whois data, but we need to keep in mind costs on registrars that, you know, that we might impose if we require them to do too much in the way of checking accuracy.

So, with that, why don't we take a ten-minute break, and I would ask everybody to come back at ten to 4:00 for the remainder of the discussion. Thanks.

(Whereupon, there was a recess in the proceedings.)

MS. MITHAL: Okay, welcome back. As I mentioned before, we'll spend probably until about 4:45 or so talking about cooperation, and why don't we spend the first half or so talking about cooperation and information sharing and then we can talk about cooperation in suspending fraudulent activity on websites.

So, I thought it might be useful again to hear from Dan to set the stage a little bit about the types of information that we would be asking registrars and registries for.

MR. SALSBURG: Let me start off by saying that the frauds that we see often involve multiple websites. So, what you will frequently see are a number of teaser sites that have some sort of claim that feed into some central sites that may be the sites for their billing, the credit card information is collected, or there's a fulfillment page where additional information would be taken for sending out the materials or for just collecting personal information that will then be traded, without the consumer's knowledge.

So, keeping that in the back of your mind, the types of frauds that we're looking at. The types of information that we see from the whois database is pretty varied. We're not just looking for the name of a registrant. We are looking at any ways that we can put together all the different elements of a scam. And that means that we frequently are trying to find websites that are registered to the same address, the same registrant, obviously, the same contacts, administrative or technical contacts, street addresses.

I alluded to before that up until several months

ago, at least with Verisign, we could search across the registrant's name field, which was a very helpful investigative tool. That unfortunately has changed, we can no longer do that. We are left right now with issuing civil investigative demands or CIDs, which are our version of administrative subpoenas, to registrars for getting information across these multiple fields.

Unfortunately, we all know, or I guess importantly, the beauty of the Internet is the speed of it. It's the ability to engage in commerce instantaneously. The downside of this is that frauds can operate instantaneously as well, and when we send out a civil investigative demand, and we get back a result four weeks later, which gives us some useful information that we can then use to send out additional civil investigative demands to other parties that might need that information, we are so way behind the fraudsters that it's getting very difficult to have in many of our cases any chance of meaningful success in Internet fraud investigations.

MS. MITHAL: Thanks, Dan.

And I think just to add to that, I think I have discussed with a lot of you in prior conversations that we often serve these civil investigative demands on domestic registrars and we get cooperation from them,

but then we have the added complication of when a registrar is located in another country, how can we get cooperation.

And I think before the break, two ideas were mentioned, Chris mentioned the idea of organizations like the FTC going through their counterparts in the other country, such as the ACCC in Australia, and then Mike Palage mentioned the idea of having a government contact list so that registrars could know who law enforcement agencies are.

I think the one issue that Dan mentions that I would like to ask everybody to think about is the need for speed in this area. And I think it's a very good point that we should strengthen our relationships with governments across borders, but sometimes we just need to move so fast. So, I'm wondering if we were to call you, one of you who represents a foreign registrar, and say, look, we really need this information very quickly, is there any way you could voluntarily respond and what are the constraints to responding voluntarily to that?

Phillip?

MR. GRABANSEE: I think one has to differentiate between the practical and theoretical side here. Certainly you can respond in an informal way and solve the problem. Especially, you know, from a Continental

European or maybe from a German legal background, was a legal system which doesn't have the threat of punitive damages, and all those things involved, the legal fees that are not as high, the losing party has to bear the expenses, it has to pay the expense of the winning party.

So, if you just give some information in an informal way, as a lawyer, consulting registrars, if they get a call from you, I would say just take a look at the site and is there some truth to what the FTC is saying, take the site away and probably nothing happens and then you can say, okay, they're never going to sue you anyway. So, it's a very practical solution.

But if you look at it from a theoretic perspective, then it gets extremely difficult. And I think that goes in the direction of the second question part of the discussion, but other agencies or agencies or courts outside Germany or outside from a different country, it is very -- there is a recognition of foreign rulings from courts or from agencies, this is a very difficult question. You know, legally you don't have a very strong meaning in the other jurisdiction.

So, if you take away a domain or give information just on a court order from a foreign country or just a request from a foreign agency, you have no

legal justification to do that. And of course you can implement that maybe in the agreement that you had with the registrant between the registrant saying we do give -- we'll provide information if we've been requested or we will cancel domain names, but then you face another problem that I think that's a point that Paul Kane just mentioned, the description of the legal relationship between the registrar and the registrant, because if you put this in the agreement as the registrant and have the justification to give out the information, you have to establish some kind of legal relationship between the registrar and the registrant, and practically, that doesn't work very often, because in between you have the registrar and then you have the reseller and then an ISP and then you have the registrant.

So, not very often do you really have a valid contractual relationship between the registrar and registrant, and for example German law, if the judge would look at this relationship he would say it's probably not valid to give justification to give the domain names away.

So, on a theoretic way, it's very difficult and probably only mutual legal aids or legal help agreements can solve this problem. But I think a practical way is if the FTC works together with consumer protection

agencies or what we have in Germany, half private, half public consumer associations, as we call them, who has the right of action, have the right to go to the United States and as an entity to go to courts.

So, if the FTC works together with those on an informal basis, works together with those entities and those groups, this is a much more effective way, because as we all know, to have mutual treaties to take care of the problem, we probably will not have before we have this established, we won't have the Internet in the way it exists now for probably only another 10 or 15 years.

But working together on this in an informal way, I think it will help and probably will be the best for the consumers.

MS. MITHAL: So, what do people think of this idea of informal cooperation?

Henning and then Willie?

MR. GROTE: Well, I have to totally agree with Phillip, because well, of course, we are of the same German experience and background. Just adding a few things to what Phillip just said. In the practical life goes with the informal way, no doubt. There still is kind of this uncomfortable feeling because while you have to know Deutsche Telekom is the world's largest teleco, we are regulated in Germany, and very strict,

and so we're always under scrutiny.

As one registrant, it might be different. It might be a different experience than that. But nonetheless, to take on the broader picture, we rely totally on consumer confidence. On that -- on the one side, it's the privacy, the data protection, of course, but the other side is a functioning law enforcement in case, just in case.

So, we, like I say, for our company, we are very, very happy to cooperate with the law enforcement agencies, and even we have installed, of course, a 24-hour hotline for all law enforcement in Germany. So, we are back now at the challenge. The whole thing, the whole issue would be much more easier and much more comfortable for everybody if we had a much more formalized cooperation. Should it be worth the example Phillip just mentioned, the kind of public/private association, whether it's a mutual treaty between the FTC or somebody else, or a multinational agreement, multinational treaty when it comes to e-commerce. There are lots of different initiatives going on on the political stage.

So, it might very well be that one of these building blocks can be used for that. So, we would be too happy to assist on that issue.

For an example, from the practical side, right now, when it goes to the usual way of legal -- mutual legal assistance, I was told by our lawyers and the data protection professionals at our headquarters that these cases usually take weeks and months to complete. And they were very, very happy that in the aftermath of 9/11, chasing an individual, everybody, the American official sides and the German ministries and all that, they were very proud that they managed the issue in a few days.

So, this is not speed. So, we would like to welcome the law enforcers. We have provided processes within our cooperation. We do have law enforcement hotlines, the only thing we need is a more formal framework. We will work informal, of course, but we need a formal framework for that.

MS. MITHAL: Willie?

MR. BLACK: Yeah, as my company lawyer would say, but as a director of the company, I would be concerned a little bit about informally giving it away. Reminding people, again, of our data protection is actually criminal. This is not just a civil -- my protection expert here might correct me, but if somebody were to challenge us, having given away their data wantonly, without doing due diligence perhaps on who was

sending in the request, then it would possibly fall as a criminal charge against the directors of the company. And I certainly don't particularly want to be taken along that route.

So, informally, I don't think it will work. I think if there was an emergency and we had some knowledge that it was a competent body that was requesting it, we might be okay. I mean, our terms and conditions say very clearly that we may provide your personal data to governmental or law enforcement agencies at their written request in connection with the conducting of any investigation.

And that's what would govern it. Of course, what is a legitimate reason? What is an investigation? We've talked about this earlier. But for sure, if you were to issue an administrative subpoena, I wouldn't know it from an ice cream wrapper, to be frank, and I don't think my lawyer would, from what she said here, because she doesn't know what a U.S. administrative subpoena is.

On the other hand, we know what something would be in the UK, and I think if you're trying to get speed here, that the best thing we could do is have a network of cooperating agencies in each country whereby the person requesting the information with some urgency

would, let's say, go to the FTC in the U.S., the FTC would correspond rapidly with the Office of Fair Trading in the UK, the Office of Fair Trading would have some means of informing us and we would know who they were. And that would mean that there would be a fairly quick path through, and you can do this by authenticated emails using digital signatures or something, and I think this might just be possible to speed up things.

MS. MITHAL: Willie, I was going to follow up with a question. I take it your point about not knowing an administrative subpoena from what?

MR. BLACK: Oh, whatever. An ice cream wrapper. I'm sure it's got a nice crust on it.

MS. MITHAL: Ice cream wrapper. I guess my follow-up question would be, let's say you know Dan Salsburg now and Dan picks up the phone and says Willie, we really need some information here, can you give it to us, and your privacy policy says we do share information with law enforcement and investigators, what would be the concern there?

MR. BLACK: If I thought it was Dan, then fine, but I don't know that it's somebody pretending to be Dan.

MR. SALSBURG: What if it was Maneesha?

MR. BLACK: Yeah, it can work, but you can set

up any pair of workable propositions, but it isn't just going to be you and me. It's going to be my lawyer or one of my customer support people that gets the first query, and it's not necessarily going to be always the U.S. and UK, it could be the Isle of Man or it could be Chechnia or Romania. And the real issue is how do we know. That's why I think setting up an N plus M, the mathematician in me, you don't want an N times M problem, because with everybody having to go to everywhere else.

So, if you can set an M plus N problem, then we all deal with our own agencies and the countries have a network between them. And then it's a three-stage process, of course, to go through it, but at least it would have some certainty, and I think we would all feel more comfortable. Because we have responsibilities. We have duties and care to the registrants that we consider very important as well. The genuine people that somebody just doesn't try to rip them off by pretending to be the FTC.

MS. MITHAL: Can I ask Jonathan to respond? And then I will call on Marilyn and Phillip and Kathy and Dan.

MR. BAMFORD: Okay, thank you.

I think I'll make a number of observations that

basically I think any arrangements which are founded on the old pall sacks, as we call it in the UK, are fraught with difficulty. I think you should formalize your arrangements in the proper contact points. I think there are areas that have to do with criminal policing and these pressing times at the moment, things could be put in place to ensure that things happen in an expeditious way.

I wouldn't believe it's beyond the wits of anybody in this room to establish quick arrangements given the modern communications which we have available to us, which apparently somebody can use but we struggle with ourselves to use in some ways. I'm sure we can manage to do that in an expeditious way through a contract where then the particular community has confidence in it being a properly routed request.

We have got plenty of experience in the UK in the past where these sorts of arrangements, where named individuals contact each other and for the exchange of information, it turns out somebody, one of the named individuals, has left the organization and is working for tracing agents and bodies like that and the information is finding its way to other areas. You might leave tomorrow for all I know, you might be sanctioned for gross misconduct, I have no idea. I'm

sure you won't.

MR. SALSBURG: But you don't know.

MR. BAMFORD: But I mean that's the point. You've got to have confidence. And a desperate action contact, even though Willie has made some statements there and the terms and conditions of which you will do business with people. He has to have reasonable grounds for believing that those conditions are met. And what's the level of reasonable grounds that he has?

Now, maybe tomorrow he might have some reasonable grounds when he gets a phone call from you, but in a month's time, I'm not quite so certain. But anyway, just anybody over the telephone without the backdrop of some official documentation is asking for trouble in any event, because you need some way to confirm just why you did it in the end.

I think a contact point in a country is a sensible way of proceeding on the basis of comparative organizations, and that strikes me as an easier way in data protection terms then because of Willie in the UK is then satisfying the demands of a local agency other than an agency in a third country who he doesn't necessarily know from anybody else. It could be, you know, the Iranian consumer protection agency are on the phone to him as much as it could be the Federal Trade

Commission.

MS. MITHAL: Thanks, Jonathan.

Marilyn?

MS. CADE: I want to first of all set the stage by saying how sympathetic I am to the problem that is faced, that the FTC is describing by sharing a situation that we dealt with right before Christmas during the shopping season when at 6:00 p.m. on Friday night, a website went up and it was called AT&T-global.net and at 6:20 we detected it ourselves and recognized it as not being a valid AT&T site.

The website was communicating with AT&T subscribers and telling them that due to a D-DOS attack and other corruption that had taken place, their subscription information had been lost and they should go to this AT&T authorized page which, oh, by the way, was a direct replica of our customer service page and fill in their personally identifiable information, revalidate their credit card numbers, and by 8:20 we had taken the site down by getting a DMCA compliant notice sent to the ISP.

By 12:00 the site was back up on Friday night. And we got it down again on Saturday morning, there was a second ISP with a second DMCA compliant notice and it went up again on Saturday night. And it was up all day

Sunday. We in the mean time had taken a number of steps to notify all of our customers, and we don't like telling our customers that they are the victim of fraud. They trust us. We don't invest in the world's tenth most well known brand for nothing. This is supposed to be a secure and reliable system that we operate.

We, of course, are very dependent, and by the way, the whois data was it appeared that it could be correct, it was a gentleman who happened to live in Ohio, oh, my God, once we found him he just happened to be in Bulgaria. The story behind this is that we are very dependent on being able to use whois ourselves, and to protect our customers ourselves, and very dependent on cooperation with the FTC and with their counterparts in other countries.

I say that and at the same time we are very cautious about informal arrangements. So, I would lend my support to the need to find a way to have an identified set of agencies. That's something, while I'm not promoting the safe harbor as a model, I might promote the concept that countries that you know in any country who to go to. If you have a company in the U.S. who appears to have violated the privacy of a European citizen, then there's a place to go for that country from the data privacy commission from the other country

can come to the FTC and there can be a contact with the country, with the company in the United States that's recognized. We know who the FTC is.

It seems to me that we ought to be thinking about those kinds of models. Is there something in an adjacent industry sector that could be built on or created in a different way, is there a way to create this network of agencies, but to formalize the relationships.

We believe very strongly as an ISP, our terms of service are very clear. If our customer violates our terms of service, we have the right to deny them service. And I think that's something that I appreciate the problem that today is registrars may have in their distribution channel, but maybe that's something that they should really think about.

If the kinds of fraud continue on the Internet that are going on now and the scams that are going on now involving domain names continue, I regret to tell you as registrars that you, too, will have to employ close to 40 people to operate an enforcement desk, and there are better ways to spend your money.

MS. MITHAL: Thanks, Marilyn.

Phillip and then Kathryn.

MR. GRABANSEE: I just wanted to make it clear

that certainly as a lawyer I am not advocating solving things in an informal way always, this is not just considering an academic discussion, also, you know, describing a little bit of reality how things can be sometimes practically solved. I just wanted to describe that certainly we would all search for a formal better structured way, especially for bigger companies who are exposed more to the public, it's certainly a problem. They will still solve problems informally but they probably won't tell in discussion like that saying how they do that.

But I have to come back to the question about the administrative subpoena, what happens if that is served with them and if it makes a difference if it's really issued from you guys or from third parties, it's not true. It might be a moral difference for a registrar who receives it, is it really a real subpoena or is it, you know, a fraud subpoena.

So, but from a legal point of view, all decisions or all subpoenas which are not recognized and enforceable by national law, legally, they mean nothing. You can accept it if you like it, you can say I accept this subpoena, I don't accept this, but from a legal standpoint, that's a problem of, as I said, recognition enforcement of foreign decisions. That's pretty much

the same in all legal systems in the world.

So, you can say certainly in your contracts with your client, if you are able to establish a contractual relationship with them, if we got a subpoena and/or if we get this from a foreign agency, we do that, you know, we would do that action, but if you don't establish it in a contractual relationship, foreign decision, whatever is legal, if it's right or wrong, if it's legal it doesn't mean anything.

That's a major problem. And if you go through this, which you can find in different treaties how this is going to happen, the acceptance and recognition of foreign decisions, if you go through that whole process, which is very complicated, they have to be translated and run through three desks and then it takes probably a half a year, at least, to get something then translated and then being enforceable in another legal system. So, this is just practical that it's the way things are. And if we find a formal way to solve that problem, I would certainly be much more happy with that.

MS. MITHAL: Thank you, Phillip.

Kathryn?

MS. KLEIMAN: As a user, I have to say I'm reassured by what I'm hearing from the different countries, and the different registrars. There is a

real concern with the registrants and that contractual relationship, which I think is important.

What I wanted to raise is that in the Internet world, everything is kind of -- reciprocity is such an important issue, and that as -- I can understand why you would be asking foreign registrars to help with speed and access, but domestically, where my domain name is registered domestically, and were the local registrars to give information on an informal basis to foreign governments, I think we would just have exactly the same problem that we're hearing the foreign registrars raise.

Because you're so -- you being the Federal Trade Commission -- are so much on top of this problem. You are very much at the forefront, I think, of the fraud enforcement that's taken place. But others will follow you, and you are in the position to kind of set the model. And I think what you are hearing is that the model should be one of process, verification, legitimate reasons, as well as speed.

So, you get to build the model. And I actually wanted to thank AT&T for setting the gold standard in this area. In the 1950s and 60s, the U.S. Government went to AT&T, as I understand the story, and said we want informal access to contents of telephone calls, and AT&T said, privacy and process are the right answers,

that's what protects our subscribers. And we had to pass laws, considerable laws about subpoenas and court orders and under what circumstances that information would be given up, and you're in the process of building the new model. So, good luck.

MS. MITHAL: Thanks.

Dan?

MR. SALSBURG: We don't have years, and that's the problem, and I think that's why I'm thrilled that you are all here. We all know that it does take years to develop these government-to-government models for how to do this. The problem we have is that in the mean time before these things are formalized, consumers are going to lose a tremendous amount of money from becoming victims of frauds.

And that's my problem here in the FTC, not necessarily yours in the CCTLDs, but you have a related problem, and that problem is that -- and we've seen this in other mediums of commerce, if it turns out that U.S. law enforcement can't do its job to protect consumers in a certain medium, that medium runs the risk of becoming a haven for pariahs, and for fraudsters, and in which case the medium fails.

And so I guess the warning out there is be careful, you don't want to have your CCTLD go the route

of certain other mediums of commerce that have just become known as where you get your psychic reading or your chit-chat with a supposedly naked lady. That's not what you want to have happen with your CCTLDs.

So, how do we deal with this? Well, in my mind, really the only way to deal with this issue is to, yes, formalize relationships, but they have to be formalized at the FTC to registrar level. That's the only way we're going to be able to achieve protecting consumers and also creating the framework for ensuring, you know, we deal with these other issues of the privacy issues in a manner that's appropriate, and I think here at the FTC, we feel that we're pretty -- we're pretty savvy to issues of consumer privacy. But, you know, we can deal with those issues, and also ensure that consumers in America are protected, and also that the CCTLD continue to function and grow.

MS. MITHAL: Thanks, Dan.

Paul, I will give you the last word on this and then I had another question that I wanted to raise.

MR. KANE: I will try and be very brief. We are all very familiar with caveat emptor, buyer beware. What I found very interesting from yesterday's debate where we were fortunate to have Mark MacCarthy here from Visa. One of the questions I raised yesterday was,

wouldn't it be better to prevent the fraud or the fraudsters from actually being able to transact.

We're in an age of electronic communications, and it's possible through various techniques for banks to notify registrars within milliseconds whether or not a card, a credit card, facilitating the purchase of a domain, is indeed valid.

Privately, or after the debate, the gentleman very kindly said, such technology may exist, but banks work at different speeds. What he was really trying to say is it's different costs. If you think there are, as we learned yesterday, somewhere in the region of 150 million chargebacks by U.S. and Canadian banks each year, and banks charge between $50 and $25 U.S. dollars per chargeback, there's one hell of a lot of money at stake if banks try and tighten up the abusive use of credit cards. They lose money.

We learned yesterday that their exposure rate, the bank's exposure rate, has fallen from ten cents in $100 to seven cents in $100. It is the merchants, it is the registrars who actually carry that. They get a refund.

One of the things I think the FTC could try and do, which would stem this problem, is to try and encourage this partnership to extend a bit more. Where

the banking system can actually share information with registrars, which will give you guys and registrars the heads-up that a fraud could be taking place, they're registering a domain name. They haven't paid for it, that's part of the gripe.

Where a registration takes place that hasn't been paid for, it's almost tantamount to fraud anyway. So, prior to registration there's a requirement for payment. So banks would know if it was going to be a fraudulent payment, the registrar would know and he wouldn't activate the domain name. So, it's quite simple.

Also in another conversation we were talking about international fraud, we're talking about cross-border fraud here. Another interesting statistic, it takes between 10 and 12 days for the international credit card service to exchange information internationally. A specific example, I am from the UK and my card is stolen here in the U.S. I will ring up my bank in the UK and advise them that my card has been stolen. It will be 10 to 12 days before my card in the U.S. is deactivated.

Now, during that time, a registration could be made, a fraudulent transaction facilitated, and for ten days the guys could be defrauding consumers.

So, it's really in the day of electronic communications, is to try and get the whole public/private partnership together such that fraud can be prevented at source and registrars aren't exposed to liability, consumers aren't exposed to liability, and working, as I mentioned yesterday, with consumer associations, FTC and the like, internationally, would actually really make a difference, but I think the banks are the key, and for obvious reasons, they aren't that keen to drop their chargeback routine in a hurry.

MS. MITHAL: Thanks, Paul.

It seems like there's a lot of consensus about the fact that law enforcement should get speedy access to information, but there are some constraints, and people have raised various constraints, and I'm wondering if we can talk about a way to move forward on these issues. People have mentioned the idea of creating government contact lists. You know, is that something maybe the OECD could do, or another body, could this discussion take place within the government advisory committee to ICANN? You know, I think law enforcement certainly would be interested in talking about these efficiencies further.

So, I wanted to get other people's thoughts on that. Michael, can I ask you about the OECD?

MR. DONOHUE: Well, the other side of the cross-border fraud coin is government-to-government cooperation, and we've been working pretty hard on that at the OECD. And it's pretty hard going. We find that a lot of our -- the enforcement regimes that are set up in the other countries don't look like each other always and can't always take to one another for many of the same reasons that the data privacy rules as well.

So, I think looking to the OECD to help formalize this role may not be -- it may not be addressed with the speed concerns that have been expressed earlier.

On the other hand, doing things like finding out contact points, that's maybe not quite so hard. We have a disadvantage of only having 30 countries that participate in the OECD. Although that's not necessarily new information, I would throw that out.

MS. MITHAL: Anybody else, ideas for moving forward?

Phillip?

MR. GRABANSEE: Again, I can only advocate, which is also a formal relationship, if the FTC would establish relationship with the consumers. Associations in various countries, however they might be organized, and establish a network working together with them and

identifying fraud or potential fraud, informing the partner organization, however this might be organized, and the organization in the country where the domain name is located, takes whatever action which is in the legal system in the country possible.

For example in Germany, if you have the consumer associations, if you see there's going to be some fraud coming from a website, which is located in Germany, or domain name, you inform German consumer associations and they go, for example, to civil court and get a temporary injunction which and then the temporary injunction is properly served and there's no concern that also for the registrar who gets a German temporary injunction, he can just follow the legal procedure and I think that's my suggestion for the time being.

Before, as we mentioned, we don't have years, you know, but we could do something. The problem is probably that the countries where domain names will be located where people commit fraud, they will not have a very established system of consumer protection, organizations that will probably not have a very effective legal system because that's why people hosted and keeps the domain names in those countries, but that's a situation that will always help, because those other countries will probably be most difficult to agree

on mutual treaties, because that's how they live and how they make their money, through those kind of people.

So, there is no clear solution to that, but working together with the agencies in the countries where they exist could certainly help.

MS. MITHAL: Thank you, Phillip.

Marilyn?

MS. CADE: I am at the risk of being somewhat controversial, I'm going to sort of suggest two things. One is I do think that the GAC, the Government Advisory Committee, at ICANN offers a new opportunity, because there's a new chair, there's a secretariat, and I think that it might be possible to explore the creation of a group of interested counterparts to the FTC to begin a dialogue about how to begin to move forward.

The second idea that I would say, at least we all ought to begin to have some beginning exploration on it. It's not a perfect idea by any means, but in the U.S., in the enactment of the Digital Millennium Copyright Act, a compromise was struck between the contact community and the ISPs and there is a procedure for an expedited subpoena, an enforcement and takedown procedure. And that is not a slam dunk.

The content owner, I'm the ISP, so let me just make sure which hat I'm wearing now, I get the

subpoenas. The content owner goes to court, there's a form that is maintained by the copyright office. They have to get a clerk of the court to stamp it. They have to present prima facie evidence there as a violation and the ISP is able to take the offensive content down based on the subpoena. That then allows the content owner to pursue other legal means.

I know this is probably not a popular idea, but in the situations where there's clear evidence of fraud, and I am not thinking that this -- I don't take this lightly, but where there's clear evidence of fraud or there are other really serious problems, perhaps we should begin to think about an administrative procedure which has safeguards, and I do say that safeguards are necessary.

I think it cannot be so simple that people would just print a copy of the format and fill in their claim and send it to the registrar. But in the case that I told you about, AT&T-Global.Net, AT&T owns the trademark AT&T, we can present the prime facie evidence that that is our trademark, and I throw that out as an idea to start thinking about realizing that there have to be safeguards and there has to be respect for national law.

MS. MITHAL: Marilyn, I think that's a really good segue into the final topic that we wanted to talk

about today, and that is the taking down of fraudulent websites.

And, Dan, can I ask you again to outline the problem.

MR. SALSBURG: Sure. Domestically in the U.S., when we sue a fraudulent operator of a website, one of the key remedies we seek in a temporary restraining order is to have the registrar pull the website down. That way there can't be any further fraud.

Clearly this remedy doesn't work as well. Okay, to be honest, it doesn't work when dealing with foreign registrars. An example of this is we filed a case a little over a year ago against a man named John Zucharini who was running a couple of thousand websites that were all slight misspellings of popular names, you know, National Rent-a-Cab sort of thing, instead of National Rent-a-Car. And these websites, a large number of them, were registered abroad.

We got a takedown order from the U.S. court, we sent copies of it to the foreign registrars, nothing happened. You know, there needs to be some way of effectuating these sorts of takedown orders, because from our perspective, whether or not a website is based in the United States or abroad, it's still having an impact on U.S. consumers.

One kind of interesting wrinkle to this is the consumer can even think that he or she is going to a .com, but be automatically redirected to a CCTLD and suddenly, you know, we're in the arena of having to figure out how to serve this order on a registrar of a CCTLD.

So, that's kind of the problem that we're having.

MS. MITHAL: And I think that this issue raises some of the same issues that we just talked about in terms of formal cooperation versus informal cooperation. But I'm wondering if it's a little bit different in that do registrars have terms of service agreements with registrants prohibiting use of websites for fraud, and could that be used as a basis to take down websites.

So, let me start with Willie and then I'll go to Mike and then Wayne.

MR. BLACK: Before you went on to this topic I was going to follow up on what was being said. In our terms and conditions, and I have to say when we set up Nominet, we focused very much on the terms and conditions and the relationship between the registrant members who are agents for the registrant, and us, and so there are three contracts basically there that you have to think about.

And under our terms and conditions, our contract says that we may transfer, suspend, cancel or amend, I've never actually tried to amend a domain name, I suppose that's change it to another registrant, but that's just transfer, upon receiving a copy of a perfected order of a court of competent jurisdiction requiring such action or where the retention of a domain name by you, that's the registrant, would be inconsistent with the terms of the perfected order received by us.

So, it is a legal term, but the question is what is a perfected order? Now, we know what a perfected order is, my lawyer will know what a UK court stamps on a document and should be able to verify that. But, again, with all due respect, I don't think we would really know whether it was a proper stamp of a U.S. court or a Canadian court or an Australian court. And that gets back to now there are means of mutual recognizing court orders, but we think that we probably would in a case-by-case basis, it depends how many of these we're going to get. If we're going to get ten a day, then we're talking back really to the economics of how you can transfer domain names. And if that's the world in that state, then we may have to face up to that.

But assuming that it was occasionally a request, then I think we would look on a case-by-case basis, and maybe we would actually investigate whether the stamp and the crest and everything that we're seeing on this order that you're sending us is really something that we can say, yes, that is a U.S. court. Maybe we would phone up somebody that we know and get some confirmation, does it really look like that. You know, we've got relationships with U.S. lawyers and so maybe we would phone up our colleagues in DC and say, you know, can you fax them a copy and is that really genuine.

So, we can do it on a case-by-case basis, but I think it would be much more difficult outside of the commonwealth companies and maybe outside the EU. So, once you start to get to some of the other parts of the world, I think it's going to be very difficult. But I believe that we would act on a court order if we could just verify that it was perfected in some way without necessarily going through the mutual court system where you have to apply for an arm's-length judgment or something.

MS. MITHAL: Mike?

MR. PALAGE: Regarding trying to work on taking down websites, there was a case that just came out, what

is it, about a week or so ago, involving Verisign. Where what happened was it was a trademark owner, brought an action under the ACPA, and the court order basically said take down the website. The domain name registrant went to Korea, got a court in Korea to say, no, don't do that.

So then the trademark owner went back to the court here in the U.S. and said, well, we have two competing court orders, and, you know, since we initiated our court proceeding first, the U.S. would trump the Korean court order, and basically in that second proceeding, the court said, Verisign registry, take it down.

So, you're very lucky, being very near to the Eastern District of Virginia, that you have a substantial chunk of the domain name .space, .com, .org, .net, .us, .bus, a lot of the registries have significant contacts in this area.

Now, let me put one little caveat here. Be careful what you ask for, because you may get it. Now, let's just take the Zucharini case. Let's just suppose you say, dear Verisign, take down these names, assuming they're, say, common net names. What's going to happen is as Willie and everybody said, the bad guys are pretty smart. And what's going to happen is, as soon as you

take down the domain name, the domain name is probably going to be reregistered after it gets through the redemption grace period or whatever procedure it must go through, and it's probably going to be reregistered in, you know, John Doe or some other name which would then potentially put the FTC back on -- back to square one, if you will, of trying to take down the person.

So, in fact, what you may want to do is when asking if you were to try to say, dear registrar, do X or do Y, you may just say please take out the DNS and sort of let the name expire its natural, if you will, death. Because again, one of the things we're concerned about here is unfunded mandates, and obviously registries and registrars are in the business of making money, and you can't go to a registry or a registrar, take a name away or don't allow it to be reregistered by anyone. It's rather difficult.

And as I said, you know, we're trying to talk about theoretical and practical, but these are some of the practical things that you need to know about in trying to tackle the bad guys, and how if you do work, if you do have this public/private sector cooperation, I think you'll sort of find ways of beating the bad guys and helping consumers and businesses.

MS. MITHAL: Wayne?

MR. MacLAURIN: Certainly for our part, again, we do things on a case-by-case basis. Taking down a domain is a whole lot easier than us turning over information. Because our terms of service also clearly state that we can -- we will do that, we will take it down and transfer it for a reasonable court of jurisdiction.

We refer everything to our lawyers, who make that determination for us, and we are fortunate enough to have a law firm that does have locations all over the place.

So, for us, yeah, great. Can we take down a website, or put it on hold? That's much easier than turning over customer information or credit card history or something like that.

MS. MITHAL: Phillip?

MR. GRABANSEE: Again, I want to make clear that it's certainly possible to solve this problem, including it in the terms and conditions, but that's taking a lot of burden on the registrars, especially the small one, because it's extremely complex to create such terms and conditions, and every legal system.

It's easy for Willie and his company with four million registrants to establish a rule like this one time and then enforce it, than for the smaller or medium

size registrar. And because it's very time consuming and it's also extremely complex because the whole system, a registrar, registrant, registry relationship, especially in the CCTLD domain space, it's really very much space on the Anglo-Saxon legal thought. So, it is possible to include it, but I have to, you know, as a registrar and consistency representative, wear that hat. It puts the burden again very much on the registrar, which already operates in a very difficult environment. But probably he has to carry that maybe.

MS. MITHAL: Thanks.

Okay, Willie, last point, and then I think we'll take the questions.

MR. BLACK: Just a very quick one. Just remember, of course, that us removing a domain name registration, or even suspending it, which is what we would say is taking away the servers and so it still remains in the register, let's say until a court finally makes a determination, we're quite happy to do that, although if it takes a long time and the domain would normally expire during that time, it gives us a little issue of whether to keep it suspended beyond the time that we would have been paid for the renewal.

But just taking it down does not remove the website. We're not talking here about an order against

the host of the web of the material. It's still there, and if they've got the right key words and everything and the Googles pick it up, the people will still find that fraudulent website, even without a domain name. So, it's not the perfect solution just to get rid of the infringing website.

MS. MITHAL: Thank you.

Last word, Kathy, and then we'll wrap up and take the questions.

MS. KLEIMAN: I get the last word? Wow.

Dan, I just wanted to reiterate something that I've raised already, which is that when you say that fraud is being committed on U.S. citizens by people operating in foreign countries and therefore you want to reach them, that sends a chill up my spine, as I know that foreign governments are going to want to reach U.S. citizens who are doing things against their laws, some of which we consider to be completely legitimate. The whole extra territorial reach of the Internet just raises such huge problems.

The domain name websites that you are trying to take down are speech, and so the more process -- and commercial speech is entitled to First Amendment protection in the U.S., not as high as political speech, but it's entitled to it. So, the more process that

surrounds all of this, from the user perspective, even though it takes time and we have to expedite it, from the user perspective, the more process that surrounds it protects speech of all sorts and it sounds like we're hearing that it protects the registrars and registries as well.

MS. MITHAL: I guess I think I'll give myself the last word and just respond to Kathy. I think that's a very good point. And I think one of the reasons why we wanted to talk about cross-border fraud and fraud in general was that we were hoping that that was at least a common denominator that fraud is against the law in all countries. And if we can kind of agree to that and then only talk about fraud at this particular workshop, I realize it raises all the issues that you raised, but for the purposes of this discussion, I think that's why we limited it to fraud.

So, we heard a couple of ideas during this half of the panel about moving forward on this. We talked about getting the OECD or another body to do government contact points that can facilitate information sharing and cooperation in this area. We talked about possible further GAC work. Marilyn mentioned an idea of notice and something similar to notice and takedown with lots of procedural protections, and I think those are all

issues that we should continue to consider.

So, with that, I would like to take any questions from the audience? Why don't we start in the back of the room and work our way forward.

ELANA BOITMAN: Hi, I had a practical question for Marilyn. In the AT&T case, it sounds like the name continued to be registered and you were dealing with just the web hosting company, which was an imperfect solution because they could easily go to another web hosting company, et cetera. Had you reached out to the registrar? What sort of responses did you get about getting the name taken down?

MS. CADE: Registrars vary in their response. That would be only one of the many incidents I could share with this audience. Famous well-known brandholders seem to be sticky, that is everyone wants to misuse their brand. And credit card fraud seems to be a real serious and growing problem for all of us.

The registrars vary. We typically would -- this happened on a weekend, began at 6:00 on a Friday night. We do take all the legal action that we can, and eventually we were able to get a temporary restraining order. We were able to identify, we had to hire a private detective in order to identify the perpetrator. And it takes us time, just as it did law enforcement, to

identify the person who was actually, and then we of course found out that he, in fact, was in another country.

MS. MITHAL: The gentleman in the tan jacket.

UNIDENTIFIED MALE SPEAKER: Just a thought, has FTC explored a relationship with INTERPOL, as we know INTERPOL is present in all the countries and that might be something to leverage off getting information that you require?

MS. MITHAL: I can take a crack at that. I think one of the things that makes the FTC unique is that we are a civil law enforcement agency and we certainly do reach out to criminal agencies, but I think sometimes the cooperation in the criminal area, the agreements that there are, the MLATs, you know, the INTERPOL mechanisms that we can't take advantage of a lot of them because we are a civil law enforcement agency.

But that being said, we do have contacts there and we are trying to build more relationships with criminal agencies around the world.

Rick?

RICK WESSON: I wanted to talk about a couple of things. First of all, when you --

MS. MITHAL: Rick, if you could limit it to one

question, I think we had other people who wanted to ask questions, too.

MR. WESSON: Okay, I'll just do one. I had several.

MS. MITHAL: We'll get back to you if we have time.

MR. WESSON: It's all right. First of all, the cost of providing services was something that was discussed. The cost of trying to identify a domain name is accurate or not, which is something that you guys have encouraged registrars to do, and I would just like to point out that the financial community, NACHA, the credit card processors, only verify a house number and a zip code in one, potentially two, countries. The amount of dollars going through those transactions is orders of magnitude higher than the entire domain registration market.

And I really wanted to understand why that the FTC was encouraging registrars to provide this service, that the registrars are a very small community, not nearly as well funded, don't have locations in the number of countries that the credit card processing do, nor the financial resources, and asking us to do something that is orders of magnitude more complicated and more costly than what financial institutions do.

And what I wanted to propose is that if we are working cooperatively, that it's the relationship

between the merchant and the credit card processor, as Paul pointed out earlier, where this could be more effective and handle more of the fraud, killing two birds, effectively, with one stone.

MR. SALSBURG: Let me take a crack at that. I think we're dealing with different types of fraud when you're talking about credit card fraud and the fraud that you see in whois registrations. What we've found in our Internet cases is that the whois data serves as the building block of our investigation. If that data is inaccurate, we have a burdensome time protecting consumers at all. We recognize that credit card fraud is awful, it's terrible for consumers, it's terrible for the merchant banks, for merchants, but from an investigative standpoint, whois data is a key.

MR. WESSON: May I ask a clarifying question?

MS. MITHAL: Sure.

MR. WESSON: Yes, could you tell us how much the dollar amount of fraud that's committed from Internet fraudulent domain names and compare and contrast that with the other financial institutions?

MR. SALSBURG: Do you work with that?

MS. MITHAL: I mean, we can talk about some statistics on Internet fraud, we just released some statistics yesterday and I would actually encourage you

to go through that and we can talk about that a little bit more later.

RICK: So you don't know the answer?

MS. MITHAL: I actually don't know the answer.

MR. KANE: Could I just follow up on Dan very briefly?

MS. MITHAL: Sure.

MR. KANE: Dan, I think the point we're trying to make is if the name is not paid for, they shouldn't be in the whois anyway. We're a believer, I think the registrar community, and the CCTLD community I believe is, in having the whois publicly available. It's good for consumer confidence, it's good for resulting technical problems, it's good to have whois publicly available. But if the bad guys are using credit cards fraudulently to purchase the web space, to purchase the domain name, to do all the stuff, if we can stop that, nip it in the bud, they'll never get on and they can never commit their crime. That's --

MR. BLACK: Please, please, yesterday we had somebody saying that the fraudsters in Canada spent a million dollars on phone bills. They're not going to worry about paying $50 for a domain name. They will pay for it if they're genuine crooks, I mean if I can say that. You know, they're actually going to be prepared

to go to a certain amount of genuine expense to rip off 100 times that. So --

MR. KANE: In which case you've nailed them, because you've got their address.

MS. MITHAL: Can we continue to have questions from the audience?

MR. CONNELLY: Thank you, I'm Robert Connelly from PSI USA and PSI Japan. This conference has focused upon cases in which consumers have been defrauded. I would like to call your attention that the majority of ICANN accredited domain name registrars are small businessmen, or small businesspersons, some even IRS section S, perhaps even sole proprietorship. None of us is a Western Union!

These small businesspersons who have invested heavily in their enterprises, most are honest, hard-working, bright citizens of their various jurisdictions.

They, too, are being defrauded.

Fraud may damage many persons all along the supply line. Will this conference agree to conclude that fraud is wrong, regardless of who are the "suckees?"

My text for the secretariat.

MS. MITHAL: I think we had a question in the

back, Commissioner Bhojani.

MR. BHOJANI: Thank you. Sitesh Bhojani from ACCC Australia. Dan mentioned earlier that one of the problems with law enforcement was to have websites shut down. Might I add that one of the other developments we're making as law enforcement agencies is also to try to get corrective measures on websites, just as you have corrective ads in newspapers or radio ads and so forth to help educate the community. One of the other objectives law enforcement agencies are looking at is getting corrective messages on commercial websites and my question is directed to the registrar community.

Dan's question was about recognizing court orders, especially from foreign jurisdictions, ordering or requiring a website to be shut down. Would you have a different view if it was a court order that required you to transfer the domain name to a law enforcement agency from a foreign jurisdiction?

Let me give you a specific example, if the ACCC wrote you a letter, tried to verify who we were, showed that we were a genuine law enforcement agency and said that we wanted that domain name transferred into our name, what would be the response from the registrars?

MS. MITHAL: Mike, do you want to take a crack at it?

MR. PALAGE: Let me. If you're going to -- I want to be real careful here. I would say, again, if we had -- I think most registrars, if you are able to verify that it was -- that you had a judgment from a court of competent jurisdiction, and I guess here is the most important caveat, that you were willing to pay for the service, i.e., the domain name registration, which as I said, you know, we're rather competitive and we offer very good prices.

The cost of maintaining a registration to do the corrective advertisement actually would probably be from a cost benefit analysis, very -- a good return on investment, because again, I think one of the things that happens, and a lot of trademark owners have made this mistake, where they'll file a UDRP, and they'll ask for a cancellation instead of transfer, and as soon as they prevail after expending several thousand dollars, the UDRP will be enforced, the domain name is cancelled and milliseconds later the name is registered by the bad guy again.

So, I think part of -- as I said, I think what you're saying about corrective advertising, you are thinking outside the box, and staying ahead of the bad guy. And as I said, if you're willing to pay registrars and registries for their services, I think that that's

an excellent opportunity for cooperative venture.

MS. MITHAL: Phillip, did you have your tent up?

MR. GRABANSEE: No.

MS. MITHAL: Okay. In the front, Susan Grant? I think this will be the last question, and then our bureau director is here.

MS. GRANT: First of all, I am from the National Consumers League and we're against fraud perpetrated against anyone, businesses or consumers, and I do think that banks, credit card associations and credit bureaus could make information more readily available to help you, and we would certainly support that.

I'm concerned about consumers' perceptions of domain names. I was talking to a college class earlier this week and asked them how they would identify a website providing information about health as a legitimate objective source of information, and one of the first answers was, well, we would look to see whether it was a .org or a .gov, but it seems to me that there's not really any screening to make sure that entities are who they are.

And then, there's the whole country domain name now. There's something up right now that I think has a name like ConsumerProtectionAgency.US, which is of concern because it has the potential to deceive not only

U.S. consumers, but foreign consumers who may be trying to contact U.S. Government with a problem, and this is, in fact, a for-profit operation. So, I would like some comment from the registrars about this.

MS. MITHAL: Anybody want to respond?

MS. CADE: Actually, I'm not a registrar, but I'll take a crack at the first one. One of the decisions that ICANN made when it introduced what is called the proof of concept around the new GTLDs was to introduce sponsored GTLDs with the idea that in order to register in that GTLD, you had to meet certain criteria. So in order to register for a museum you have to be a museum and you have to present your credentials. And in order to register in .aero, you have to be affiliated with the aeronautics industry, et cetera.

I think one of the questions that is still being debated and the evaluation that's going on is is that a good way to expand the name space, and does it bring some relationship between the name that is between the TLD and the entities who are registering in it.

Beyond that, most of the TLDs are -- that are available -- are open in one way or another and the criteria for that is really not in the hands of the registry or the registrar, but is set by ICANN policy.

MR. PALAGE: Okay, a couple of things. First,

with the .US, that is operated outside of the ICANN regime, that is a CCTLD, and you have -- you're fortunate enough two rows behind you is Jeff Newman from Newstar, the registry administer for .US, so you may want to contact him, and as I said, myself being a policy member of the .US Policy Council, the U.S. Government, I think, does have an interest, I mean, they do have certain safeguards regarding trying to maintain the space in a productive manner, and as I said, that's something you definitely want to try to communicate.

Getting back to what registrars could do, I think Bob during his statement really hit the nail on the head that there are a lot of small to mid-size registrars. If you look at it from a numbers standpoint, let's just say there are 30 million generic TLDs in the name space. If you look at the top 20, the 20th has 200,000 registrations, so the other 140 generally are dealing with thousands. And, again, these are small to mid-sized businesses that are not in the business to be a content policemen.

I work with a number of registrars that get calls that say, well, this is child pornography or this is that. You know, again, and it's rather difficult. You know, again, most registrars, I think, are responsive, they try to work, you know, with law

enforcement or they do try to respond to most valid queries, but I don't think that they are in a situation to take down ConsumerProtection.US, you know, again, that's sort of where you need to work with your counterparts here, you know, the people at the FTC to try and identify something and take it down that way.

So, I think that would probably be the best registrar situation or best generic registrar response. We're not content police.

MS. MITHAL: Okay. Kathy?

MS. KLEIMAN: I think the college students have a real challenge and if they understood the difference between .org and .gov, they're doing pretty well. The .gov sites are -- I mean, that would be a place to go. That's not an open GTLD, that's the U.S. Federal Government. They understand, they're beginning to understand the differentiation.

But this is the big question, one of the big questions for users on the 'net is, whose news website do you trust, where are you getting your news, where are you getting your health. We can't ask ICANN or the registrars of the registry to be the speech police.

Part of the wonder of the 'net is that everyone can participate. People are going to have to learn where to get -- this is where third parties, people are

going to come in and tell us who's speaking, but please don't ask ICANN or the registrars or registries to do that kind of speech policing. It's not fair and it ultimately isn't right.

MS. MITHAL: Well, with that, we will conclude that panel on cooperation between enforcement agencies and registrars and registries, and I want to thank everybody, particularly those people who traveled from far away to be here, and I want to thank everybody for a very lively and interesting panel.

(Applause.)

MS. MITHAL: Now I would just like to introduce Howard Beales, who is the Director of the Bureau of Consumer Protection, and he will just make a few concluding remarks about the conference.

MR. BEALES: I want to thank everybody for coming and for some very informative and very productive discussions over the last few days. And I wanted to especially thank all of you in light of our own very cross-border problems where cold air from Canada met warm air from the Gulf of Mexico and produced blizzard '03. I want to thank Stacy Feuer and Tara Mikkilineni, who are really the keys of putting this together and doing so despite some pretty difficult conditions at the end, particularly given the snow problems.

I want to encourage anybody who is interested to submit comments in writing, if you didn't have a chance to say something here, then send it to us in writing, and we will, of course, we will of course consider that. But I think it's, you know, it's particularly useful since there may have been people who wanted to be here and couldn't make it.

I did want to highlight a few key points I think that come out of the workshop and that are areas for further work together. First is I think a very general recognition that cross-border fraud is harming consumers and harming legitimate businesses. It imposes costs in terms of dollars, it imposes costs in terms of the resources that we devote to fighting fraud as economists are fond of saying, part of the cost of crime is what we invest in locks. And it imposes cost in loss of consumer confidence and in damage to reputation.

Second, there's obviously a role for vigorous law enforcement from the FTC and from criminal law enforcement authorities, and that's help, but more needs to be done on a systemic basis to try to curb the problems rather than rely simply on after-the-fact enforcement.

Third, I think it's been clear that the private sector is willing to help and has acknowledged the

importance of speed in dealing with cross-border fraud. It moves quickly and we have to, too, if we're going to make any difference.

Fourth, I think the keys to successful public/private partnerships are concrete objectives that we want to accomplish in clear, well-understood divisions of responsibilities. We need to make best use of the information and the resources that we each bring to the table. We don't want to ask private sector businesses to become law enforcers, or to assume broad, unfunded mandates, but we do want to ask you to contribute the tools and the information that you have to what really is a common cause.

And I think a final key is working across borders. For the FTC, pairing with consumer protection law enforcement agencies in other countries, for the private sector in working with affiliates abroad, so that a public/private partnership really can work across borders just like the fraud operators that we're trying to pursue.

I think there's also some specific areas of agreement that are applicable to all of the private sector participants, and some industry-specific points that I think are worth making. I think there's a consensus that there's a need for some sort of broader

information sharing, that that's one thing we can clearly do and as well as training and business and consumer education. I think we can work on those things.

In particular, I think government and private sector can do a lot more to put in place mechanisms that maximize the speed and timeliness of information sharing, and that minimize confusion and delay. We can appoint agency liaisons with private sector organizations. We can put together resource lists of private sector representatives who are working on cross-border fraud and security issues. We can have law enforcement work together to set up referral points for information that's coming in from the private sector. We can develop ways to identify the right agencies for the private sector to contact and cooperate with in particular matters. And to authenticate that you really are dealing with somebody from that agency.

We certainly don't want our identity stolen. We can use companies' internal communication systems to share information about the latest frauds and about enforcement needs. And we can set up training sessions so that law enforcement understands the way that business operates and the best ways to frame requests for information, and so that companies understand the

way the FTC works in our civil law enforcement investigations. You certainly don't want to find out by being a target.

Turning to some of the specific industrial areas, or business areas, in the financial sector, I think there's a consensus that information from some of the very sophisticated tracking and risk assessment techniques and mechanisms that are already in place would be valuable to the FTC. I'm certainly convinced. I think that would be extremely useful for us to be able to access, use, understand consistent with your needs.

And I think for payment systems, there's some fairly clear agreement that some mechanisms that are already widely used, such as fraud alerts that are circulated by the credit card industry, can be expanded to include the FTC and hopefully to facilitate reducing the problem. And I think more consumer education, including at the point of purchase, is something that may also be helpful.

In particular, we would like to follow up on the suggestion to look at ways to have industry analysts work with law enforcement to analyze data we currently have available. How can we make better use of the complaint data we get to select targets, and that's something where there's a lot of expertise in this room

that unfortunately doesn't work for the FTC.

For commercial mail receiving agencies, and for courier services, I think expanded training for operators and courier agents who deal directly with consumers is something that could be a very useful tool. In particular, I would like to thank FedEx and MBE for their offers to follow up in this area. I think that's something that would be quite useful.

And for ISPs and web hosting companies, I think there was agreement that it's important to be able to act quickly on information preservation requests, and to consider whether we can find a way to pass on preservation requests to the next organization in the evidentiary chain. There's interest in using companies' terms of services -- terms of service -- both to address privacy concerns, and to stop websites that are determined to be fraudulent. And I think there's some interest in developing a vehicle for consumer protection agencies in various countries to work cooperatively to obtain information from companies that are outside of their jurisdiction.

For domain registrars, in particular, I think I heard some agreement, that there should be a way for legitimate and verifiable law enforcement agencies to get access to accurate whois data. I recognize that it

has some costs, but it's the essential first step in knowing who it is that we're investigating and where to go.

I think there should be streamlining of requests for cooperation from law enforcement to domain registrars and to registries. We should try to utilize identifiable points of contact with you all, and with law enforcement agencies around the world.

I think it's interesting that a concern cutting across all the panels is the interface with privacy laws. I think information sharing and information utilization is a key to the fight against fraud. I think we need to focus on the ways that information is used, and there's some good uses of information, like fighting fraud, where we should strive to not let privacy regulations get in the way. And we may need to work together to find ways to harmonize the need for that greater flow of information, with privacy schemes in various countries.

In summary, I think this workshop demonstrated there's a very real and very important need for public/private partnerships to combat cross-border consumer fraud. There's a lot of details to be hammered out, and a lot of issues that still need to be decided. But I think this meeting put us one step closer to

creating ongoing and productive partnerships.

We look forward to continuing to work together on the issues and the ideas that have been generated by this workshop. And, again, I want to thank you for your contributions of your time and your effort and your attendance. Thank you all very much.

(Applause.)

(Whereupon, at 5:15 p.m., the workshop was concluded.)

- - - - -