A TRANSCRIPT OF

FORUM ON CYBERCRIME PREVENTION ACT OF 2012

Hosted by Office of Cybercrime-Department of Justice and Information and Communications Technology Office-Department of Science and Technology
09 October2012

Emcee: Good morning everyone. May you please rise for the induction by, invocation, I'm sorry, by Mr. Ronald Aguto of the National Bureau of Investigation.

Mr. Aguto: Almighty Eternal God, we thank you for the miracle of life and for all the good things that you have given us. Send your spirit upon each of us as we conduct this forum on Cyber Protection Act of 2012. Give us the gift of understanding, knowledge, and wisdom, that we may be enlightened and informed about the topics to be discussed today. This we pray and ask for your mighty name, Amen.

Conductor for National Anthem: Please remain standing for the Philippine National Anthem. Bayang magiliw, handa awit… (All sings)

Emcee: Thank you. Please be seated. And to give us a brief introduction of the event, may we please call on the current chair of the Committee on Information and Communications Technology in the House of Representatives, and represents the second district of the City of Taguig. This gentleman believes that technological innovation coupled with education reform and social transformation will turn the world upside down and will allow for the small to take on the big, for the smart to beat the strong, and for the nice guys to finish first. Ladies and gentlemen, please help me welcome Congressman Freddie Tinga.

Cong. Tinga: *Maraming, maraming salamat at magandang umaga po sa inyong lahat*. Thank you for having me here. Usec. Louie Casambre, Asec. Sy, Mr. Dondi Mapa, my former boss. *Sa lahat po sa inyo ay isang maganda umaga at maraming salamat po sa inyong pagdalo*. You know this has been a talk of the town for the last couple of days, couple of weeks, and it's very good and very timely that a forum like this has happened and we get to talk about the meat and potatoes of what anti-cybercrime really is all about. And at the end of the day, it's all about technology, and we talk about technology in the sense we talk about a lot of other things, that it can be used for both good and bad. *Parang kotse eh*. You know when they came up with the car, it's said that you could use it to go from point A to point B or you could use it to run over someone. It really depends on who's driving the vehicle. So who's driving technology and what are the guidelines that are put in place to make sure that you use it to go from point A to point B rather than running over people? The anti-cybercrime law, as we've said before, this is my personal opinion noh. And I've stated this time and again, was antiquated even before we wrote it. And that's because that's the world we live in. Talagang ang bilis ng pagbabago and if you are going to count on the laws to catch up with technological change, you will be sadly disappointed. We're playing catch-up here; the laws are only as good as the people who will implement them and the thing to understand about what these laws are at the end of the day, pantulong lang 'to. If you look at technological change, it's really the business models that are affecting industry and the various sectors that make up an economy in the society we live in. *Tignan niyo na lang yung nangyayari*. I mean you look at the kind of laws that we put in, *sabi nga dun, merong nag-ahh, merong nag*-tweet or *nag*-post *sa* Facebook, *sabi "Naku pano yan*?" And this is for you, Mr. Dondi Mapa. *Binabasa ng asawa ko, sabi nung* tweet *"Naku! Pano yan? Kelangan na* original *na yung* Windows *ko*." You know the point of it was that, *dapat naman diba*? But then again, and I'm not gonna wait for you guys to answer this question, and I don't want you to answer this question. You think about it, who here has not downloaded a music MP3 file? Who here has not used an unlicensed version of

software? *Ang babait niyo*. But that's the nature of the beast. So even without the law, what has happened? You look at music industry professionals; you look at performance artists; why are they all of a sudden going all around the world performing in concerts? *Kahit dito sa Maynila, bugbog tayo ng* concerts. *Bakit? Kasi hindi na sila kumikita sa* record sales. You look at the software industry and you look at companies that are pushing what are called free or premium models. They've changed the ball game. Again, a reminder to software developers, if you are counting on revenue stream simply from the license sales of your software, mahirapan kayo. You have to rethink the industry.

Encyclopedia Britannica is printing its last physical encyclopedia this year. Most probably because of a thing called Wikipedia. So it's not the loss that changed things, it was how people were reacting to technology. So I think that's a guideline for everyone to understand that we put laws in place to a large extent some of the provisions probably are antiquated. But they do help us, guiding us into where the future would be. I guess a few reminders of what cybercrime is and isn't. When we drafted this and you can see the version of the House and the version of the Senate were quite markedly different. The House probably saw the law very differently from the Senate and the version that came out was a combination of both. I have to say as the chair on the House's side, not every provision there was to my liking, but that's what you get in a bicam. Give and take *iyan at kaysa lumabas kang* obstructionist, *meron kang palulusutin at meron hindi*. The items that came out and have been talked about extensively: libel, libel. Libel, as far as we knew was illegal, if defined properly in the real world. And so the point of the House was that anything that was illegal in our real world, you move it online, it's the same thing. Talking to Asec. Sy many months before, *pinag-usapan namin to* and he was consistent with the position, "*Huwag niyo nang lagyan ng* particular clause *yan dahil nakakagulo pa*." *Tama ka*. Because a simple explanation that is if it was illegal in the real world, it should be illegal online. And following that, if it is legal in the real world, it should be legal online. So, *kung titignan niyo yung* converse *nun, walang dapat katakutan. Kung walang mali kayong ginagawa sa* real world*, huwag kayong matakot na yun rin ang ilabas niyo* online*, dahil wala ring problema*. Let me give a case in point and this is not to make a political dig at my opponents but to explain why there should be very little to fear from the right implementation of the cybercrime law. *Kaya nasa sa inyo yan sa mga mag-i-implement*. In the City of Taguig, the nurses at the city hospital were complaining about the mismanagement of that particular hospital, I think this came out in the news. So one person posted a criticism of the hospital administration and the way the city was handling the hospital. *Hindi na po ako yun nagpapatakbo ng* Taguig *so hindi po ako yun*. And a lot of that nurses, they liked that comment. And as a result, the nurses were relieved from the Taguig city hospital. Ang sabi ng mga nurses "*Bakit kami pinalitan, ba't kami tinanggal? Eh nung kami nag-like sa* Facebook, *wala pa naman nung* anti-cybercrime law." The reason I'm saying this is because there was no connection between the city's mismanagement, and intimidation and harassment of their nurses, and the cybercrime law. *Walang koneksiyon iyon*. It was the way the city handled the situation which I think was wrong but it had nothing to do with the anti-cybercrime law. So it is a brave new world we face. Some of the issues that media and people have raised with the cybercrime law have to be tackled in the implementing rules and guidelines to be prepared, and we would definitely invite media to be part of the development of these guidelines. One particular section I'd like to mention that if taken by itself, *nakakatakot nga, nakakagulat*. I believe it's Section 19, which seems to say that sites can be taken down. So *parang* SOPA '*to*, *parang* PIPA *sa* US, which we were very, very much against. That if you read the whole section and this is what we have to clarify, that data can be blocked only when it has been… the case has been filed, evidence has been presented. So *talagang may violation*; not on the whim of any one person, any one department, any one agency. We were very clear when this bill was being prepared but there have to be proper checks and balances just as there are in most other things in life. I said it at the start of this introduction and I'll say it again, technology is a tool and as we go into a brave new world, you'll see a very, very different environment for all of us. We've talked about this, we've said these kids are not gonna get the education in a classroom; people are not gonna be working from offices; people

are not gonna be getting their news or their entertainment from the newspaper or TV in the near future. You won't be using banks for financial transactions; government will be outsourced. So you're gonna see all these changes and I urge everyone here when they look at technology as that tool to use it for good. To use it to make the world a better place because we've seen at no other time in human history can one person change the world for the better. *Sa inyo pong lahat maraming, maraming salamat. Magandang umaga. Mabuhay po tayong lahat.*

Emcee: Thank you very much Congressman Tinga. So before we proceed, just a few house rules please. Can we please turn off our cellphones or at least turn them into silent mode for the duration of the event. And, we would like to recognize our guests and may we please request you to stand up to be acknowledged. So we have representatives from government to be led by, of course, Undersecretary Luis Casambre, good morning sir; Undersecretary Francisco Baraan, good morning; Director Nonnatus C. Rojas of the NBI, and of course to the rest of the NBI team with you sir, good morning. And then we also have representatives from the private sector like the PhCert, ahhh, I don't see anyone of them yet… oh yes, Sir Lito Averia, good morning. We also have representatives from the National Defense College of the Philippines. We have Foundation for Media Alternatives; representatives from PhNet Foundation; Department of Science and Technology. We also have representatives from the Imperium Technology and the University of the Philippines; ICTV; UP College of Law; may we please call on Atty. JJ Disini, good morning sir. We also have Assistant City Prosecutors from the DOJ and from the PNP, we have Colonel Sosa, Major Yubra, good morning sirs; representative from the OSG. Okay… We have also someone from the Information System Analysts; National Defense College. We have Parole Probation Authority; IDEACORP Phils., good morning. Okay, from the Bureau of Immigration, good morning. From the Casiño, Celis, Hernandez, and Associates, Mr. Eduardo Casiño, good morning. I-Concept Global Consultant, Mr. Owen Cruz…. We also have someone from the Human Development and Poverty Reduction and the Commission of the Human Rights, good morning. Of course, I would like to thank the Landbank for lending us this beautiful venue that accommodated all of us. I hope you are all very comfortable at the moment. And may we also share with you that we are on live-streaming via the NowPlanet.TV and you can access us also live at the DOJ website, doj.gov.ph. And for the duration of the forum, please feel free to send us your questions at the… it's flashed over here: at cybercrime@doj.gov.ph or you may text it at… and we will gather all your questions and address them at the open forum at the latter part of the forum. And just a quick rundown of the forum for today, we will start briefly with the introduction and review of legislation, and then a presentation on the salient provisions of the Cybercrime Prevention Act of 2012. We'll have a short break after that and then we'll proceed to the open forum in which questions will be necessary. We'll have a summary and action steps towards the closing remarks.

So, without further ado, let's start with the first presentation. Our speaker has served as president of the prestigious professional organizations. He was former president of the UNIX Users' Club of the Philippines and the Philippines Association for Open Communicating. He is Microsoft's National Technology Officer for the Philippines and also the president of the Infocom Technology Association of the Philippines or ITAP. Ladies and gentleman, please give a warm welcome to Mr. Damian Domingo O. Mapa or Mr. Dondi Mapa.

Mr. Mapa: Actually, I'm just the intermission number between Congressman Tinga and Asec. Sy. I was asked to talk about the history of this Cybercrime Prevention Act. Before I start, I'd like to acknowledge the presence my former colleagues in government, Secretary Ray Roxas-Chua, formerly the chairman of CICT; and of course Undersecretary Timmy DST Rivera, former Director-General of the NCC; Is Ivan here as well? Sec. Ivan Uy, not yet? I believe he's going to be here for the Q and A portion. He'll answer all your questions.

I'm here to warm you up for the main event, right, Asec. Sy? Just by way of making this more interactive, I'll have a short survey. Just please raise your hand if you feel that A - We need the cybercrime legislation and what we have now is perfect. Anyone? If you raise your hand now you can already go home. B – How many of you feel that we do not need any cybercrime legislation? So if you didn't raise your hand for A or B, then you're probably in C. We need cybercrime legislation but some changes are needed. Raise your hand, please. Okay. Alright, so we're clear where the audience lies.

As a further question, I would just like to get a feel of where, where you're coming from. I know where JJ's coming from. We know we have several others that have been quite vocal about their positions. But just for today's purposes, we want to control the open forum a bit later on and want to address really the pressing questions. If you could just ask one question today about Republic Act 10175, would it be on the provision on online libel? Would it be about the higher penalty for crimes using ICTs? Would it be about the warrantless collection of traffic data or Section 12? Would it be the seeming double jeopardy where you can be brought to court for online libel as well as for libel in print? Would it be Section 19, blocking or restricting without a warrant, any access to a website based on a prima facie evidence. Or would it be question on some other position? So again, that is important because we'd like to know how to run the open forum later on. How many are going to be asking a question on online libel provision? How many will be asking on the higher penalty clause. How many will be asking about Section 12, warrantless collection of traffic data? Okay. How many will be curious about the double jeopardy? Okay, quite a few also. And how many are interested to ask about Section 19, the blocking or the warrantless seizure? Okay. Any others that we missed? Yes. Janet, what are you going to ask? Ah, okay. Very interesting. This is, sorry, but this is a live broadcast. Maybe, Atty. Rudy, yes, what are your additional questions about? On the constitutionality? Okay. I think sir, you lost your way, the Supreme Court is over there. Just kidding. But that's right. If we have time, we can get to some of those. Thank you.

Now, you know, when I was asked to talk about this portion, they told me, talk about the legislative history of the bill. I said how far back do you want me to go in terms of legislative history? And I asked myself, why do we really need laws? They're really there to regulate human behavior. Actually, from as far back as 4,000 years ago. For example, the Code of Hammurabi which states, if anyone steals a property of the temple or the court, he shall be put to death. So the crime is stated as well as the punishment. But there's also this concept of a heavier degree of punishment. Like, if you strike… law 195 of the Code says if you strike your father, your hand will be cut off. If you strike someone else, that's okay… they'll whip you or something. But if you strike your father, your hand will be, shall be hewn off. They show the society at that time wanted to show greater respect for family values. So there were these special circumstances that were introduced. Another law that is over 4,000 years old is the law referred to as the Pentachu which contains the 10 Commandments associated with Moses in the Exodus story in the Old Testament. I bring it up because it is interesting to look at the 9th Commandment that states those shall not bear false witness against thy neighbor. Does not say in media, in print, or online. It's basically covering all types of media. So as you can see, the human race has a rich history of having legislation aimed at regulating human behavior. How about in the Philippines? We have had similar codes. Beginning with the barangays before the Spaniards came. And then of course the Spaniards gave us our first, you know, code from 1886 to 1930. So even after the Spaniards left, we continue to use that. Then we had the penal code first enacted in 1930, amended since many times over so we now call it the Revised Penal Code. All of the things that we notice in the Revised Penal Code is that it also contains this… you know, state the crime, state the punishment. But there are cases when there is a heavier punishment that is meted out. These are called aggravating circumstances. For example if you commit a crime during a time of earthquake, calamity or other misfortune, your penalty is higher. Why? Well probably you can already reason that out, *noh*? People were already suffering *tapos* you give them *pa* heavier suffering. If you commit a crime with the aid of persons aged 15 or below, again, the penalty that's given to you for the crime is higher. Okay.

Why? Because we value our youth, we should not be subverting them to evil cause. We should actually be helping them. Why use them in committing a crime? Very interestingly, it also says, if crime is committed by means of motor vehicles, watercrafts, airships, or other similar means, then your penalty is higher. You notice here the concept where there's a new technology that's introduced, and that technology is supposed to be used for the good of society. And if some people use it for a crime then we punish them. Of course, you also punish them because it's harder to run after them if they're... take note at that time, the policemen were probably on horses. So they said, "Well if this guy uses a motor vehicle and he keeps getting away, when we catch him, we should put him in jail longer. Alright. I'm not saying this to support the concept of higher penalties, I just want us all to be on the same page and have a shared context, whether you're looking at this legislation for the first time or for the one hundredth time.

So what is really the nature of cybercrime? First of all, it's fast. It can be done in a matter of milliseconds. Ask yourself, if you're a carnapper, how many cars can a carnapper steal in one day? Maybe three, four. I know if you're Nicholas Cage in this movie "Gone in 60 seconds", you got 60 cars, right? But a typical carnapper, how many can he carnap in one day? Compare this to a cybercriminal. How many victims can he have in one hour? Hundreds of thousands, probably. Second, cybercrime is random. Doesn't matter whether you're old or young, or you're rich or poor, or a student or a journalist, you can be targeted by cybercrime. Unlike when you're walking down the street, and probably the criminal is observing someone that he can rob today. "Is his car nice or not?" Here, it does not matter who you are; you can be targeted for cybercrime. And yet strangely enough, you can also be targeted specifically. What do I mean by that? If someone were to go into your bank, open the vault and steal the money there, the bank cannot say "Oh, Mr. Laggui, you have an amount of one thousand pesos stolen from your account, and also Mr. so and so," you cannot. The bank's money was stolen. When we talk about cybercrime online... in the US where they've been getting statistics about this, over 500 million dollars of funds that have been repeatedly stolen can be traced to individual account users. So when a cybercriminal steals money from a bank, its steals from your account or not just from the banks account. So it can be also targeted. It's anonymous. You have no idea who did it to you. You've no idea who to run after. Hopefully you're going to rely on the law which has the powers to now run after cybercriminals and they're going to do it for you right, to keep you safe? And these attacks are also persistent and pervasive. They're happening every minute of the day. Whether you're at your... as long as you're logged on, malware can be working on your computer. In fact, If I were to do a quick survey here, I'll you how many times have you ever met the real criminal? Or how many times have you been a victim of a crime in the real world. Probably, many of you will say maybe once, twice. My wife who has lived for 50 years, she said... please censor that comment. She's lived, my wife... okay, never mind her age. My wife has been victimized three times in her entire life. But I asked her, "You know darling, you know how many times that you're attacked by a cybercriminal? Probably hundreds of times a day." But you just don't realize it. Sometimes you see it, sometimes your screen flickers, sometimes you're re-directed to URL, sometimes this message comes on which says you have a virus or you have to call the administrator. Of course the administrator comes, puts in his password, then suddenly your network is open to attack. You get pictures; you get emails saying here's a picture of this or that. That's already someone that's trying to break into your system plus it's inconspicuous. The nature of cybercrime is that some oftentimes, you may not realize that you have lost your password, that you have lost your files, until days or months later. And by the time you realize that the crime has been committed; the criminals have gotten away. And so one key message is that if and when we do catch these cybercriminals, let's try to make it a little bit harder for them also to get away. So if we were to look at our awareness and how we've tried to legislate human behavior in the area of cyberspace, of course, we have this period from 1999 to 2004, which we can call our awareness period. We actually had a first draft to the cybercrime law even before the E-Commerce Act. Many people here have worked on them, on those drafts. I know they were mentioned earlier.

We were not able to pass a cybercrime bill in the 12th or 13th Congress but we were able to pass the E-Commerce Act which is the Republic Act 8792. And we also had Republic Act 9208, the Anti-Trafficking Act which covers the use of ICT's to traffic child porn. So at least these are already the building blocks of legislation to come later on. We saw several cybercrimes reported but really these are just a handful, less than 5. When I joined the CICT in 2004, we started to see that many more crimes were being reported. I can tell you, I can stand here and talk to you for hours about all the crimes that we started seeing reported, phishing incident, scams, and hacks. In fact in this period between 2004 and 2010, we saw the Hayden and Katrina scandal, who can forget that. And so there were two new laws passed: 9725, the anti-child theft, you know 9208, and we have law 9995, the anti-voyeurism law. So you start seeing the trend. When you see the errant behavior, we put up an act to control that behavior. Most important thing about this period 2004-2010 is that, we decided that there was a need for data privacy legislation. Because at that time, data privacy had been covered in the, in the anti-cybercrime bill and we are also using a DTI ordinance to regulate that. But we saw that quite clearly there was a need for another bill just to cover data privacy. And so those two drafts were submitted, and finally we now have the bill of cyberspace legislation, 2010 onwards. These were almost passed in 2010. By the way, the 14th Congress failed to pass it, so the 15th Congress finally passed 10173, the Data Privacy Act and 10175, the Cybercrime Prevention Act. So in closing, this has been quite a long history. But I just want to give us all the appreciation of what has gone into these bills. I like to also remind us that in order to get the big picture, we really have to read these bills back to back, just like when you look at the Revised Penal Code. You have to look at all the amendments attached to it that have added new types of criminal behavior to the RPC. And so on. We look at the Cybercrime Prevention Act, I submit and I would like to use this in closing to say that you cannot read the Cybercrime Prevention Act in and of itself and just judge it that way. You have to also look at, for example Data Privacy Act, which tells you as a citizen, as an internet user, what are your rights to the data that you have. So I'll like to end there. Thank you for your attention and I know you're all waiting for the main act. Maybe I'll call Kat to come in to introduce our next speaker. Thank you.

Emcee: Thank you again Sir Dondi for that. Before we proceed, I would like to acknowledge the presence of our Solicitor General, Atty. Francis Jardeleza, please stand up sir. Good morning, sir. We also like to acknowledge the presence of Retired General Rex Piad of the Special Envoy for Transnational Crimes. From… representative also from the National Security Council, Mr. Reynaldo Ola. Okay. And a few more guests from the private sector. Just a quick rundown again. Mr. Benjamin Barretto, the executive director of the Foundation for Media Alternatives. Mr. Horacio Cadiz, from the PhNet Foundation, the executive director also. Mr. Francisco Magno, director of the La Salle Institute of Governance. And of course, our Prosecutor General, Mr. Claro Arellano. Good morning sir. Okay. Deborah Nga, vice chairman of the Asia Internet Coalition. May we also see Mr. Rodolfo Salalima, SVP for Corporate and Regulatory Affairs of the Globe Telecommunications. And from the Office of the President, Mr. Ordoñez, if you're here. From the Department of Interior and Local Government, Ms. Maria Elena Robosa. Good morning ma'am.

Okay. So last year if you will recall, we had around 90 days to, the Department of Justice rather, had 90 days to prepare the First Justice Summit that was held at the Manila Hotel. And that was history. And now we are again making history because for just 2 weeks, we tried to gather everyone from the private sector, from the government sector. Of course, our media partners as well, for this forum on the Cybercrime Prevention Act. And the person who spearheaded all of this, of course, is no less than our head of the Office of the Cybercrime. Please help me welcome, Assistant Secretary Geronimo L. Sy.

Asec Sy: Good morning everyone. It's going to be a 36-slide deck of presentation and you can help me with the slides because we've cut it up into slices of three (3) portions of twelve (12) decks each. One is on IT, for the IT people; the next set of 12 is for law, for legal people; and the third deck is on policy, for policy-makers. But the real challenge is

that we've mixed all the twelve (12) slides together into a slack of 36. Hopefully, we can address some of your questions. So for the next session, about 30-40 minutes, I'd like to keep it very short and crisp. One is, I'd like to give you a short overview. Second, instead of doing sections of the law section by section, we just go straight to the heart of the matter: Section 4, Section 5, 6, 7, 12, 19, 20. Hopefully that will cover up all the questions you've raised. Of course, you are free to comment now or after. And towards the last part of the 10-15 minutes of time allotted, we will talk about some of the challenges in implementation. After all, we are all concerned about how the law is supposed to be implemented. Okay. Ready? Good.

So this is now the title of the presentation. This is a long tag line but this is now the Office of Cybercrime which was constituted just on October 3 and I was formally appointed also on that date, the new Office of Cybercrime. Hopefully, this will bring our crime fighting tools, crime prevention, to the twenty-first century. And the whole point is to go against transnational organized crime, criminal syndicates. As a matter of priority, let me say it on my lawyer's oath: blogging, individual comments, tweeting, boyfriend-girlfriend discussion, those are not the priorities of the Department of government. It is very difficult, as it is, to catch fugitives from justice, what more individual tweets and individual likes. So let's manage our expectations, let the law work, and see how we can manage the new law to the implementing rules and regulations. I have a very special announcement towards the end of the presentation. Okay. And thank you Dondi for the quick presentation. At least that gives me a head start. This is now the Internet world. I don't wanna beleaguer the point. So we go on the next slide, and I just wanna summarize earlier what we talked about. The emergence of cybercrime is beyond question; the substantial difference between physical and virtual worlds; and of course, the reach, accessibility, and the convenience of doing it. And the question becomes: are you more likely than not to do or say something wrong or bad if you're online compared to when you're in physical world. That is the first question we have to ask ourselves individually.

More likely or not, if it's the same, then there is no substantial difference. But you and I know that if you're sitting behind the computer, online, fast internet connection, there are different dynamics that come into play, and first is a sense of permanence. Let me go back to this concept of permanence in a bit. And then the need for law regulation which I don't think is anything that needs to be argued or discussed about. So in '07 the Department of Justice conducted our First International Cybercrime Conference. Some of you were there and we had such a different time passing a set of ICT laws including the DICT and all that. So we strategized and said "Why don't we come up with three-pronged approach?" And the three-pronged approach now is what you see, the Data Privacy Act, – 10173. Of course there are certain issues there. Now cybercrime – 10175, and then cybersecurity. And so this one seems to validate the strategies taken in '06 and '07, that instead of lumping all the laws together and for legislators and everyone to have difficulty grappling with privacy issues, cybercrime, internet, why don't we just managed the process and cut it up into three portions. So our simple advice is when you're reading one particular part, read it in conjunction of the whole thing. We said, "Let's declare private first; let's declare sanctity, sanctuary for certain information. Then we'll talk about criminal behavior, then talk about cybersecurity." Okay? At least we have two out of three. And regardless of what happened, we'll not talk about insertions, or who's responsible for what. It's a whole government responsible, it's a whole society responsible… But personally, I would like to thank Congressman Tinga who has been a number one supporter of the DOJ and the Technical Working Group. And as I always say, it was already done. So his is how where we are now.

Okay. From the time that we had the "I love you" virus, we already set up our cyber forensics laboratory, and the basic idea of cyber forensics laboratory is that if you have

DNA sample, blood samples, even samples for rape, you would also need cyber forensics. How would this be channeled? How you analyze certain log data? How would we go about introducing evidence in this regard? And we're very happy that we have basic forensic capability today. Of course this is an ongoing effort, we will continue to upgrade. And then we also had our first conviction, courtesy of the PNP-CIDG team. This was under Section 33 of the old, of the E-Commerce Act. So in the context of the Revised Penal Code in 1932, which is the general penal code that we have, 1960's we started this process of "special penal laws," the criminalization of certain acts which is not covered by that [Revised Penal Code]. So you put that together, it now becomes this portion here and that was the trend all the way to 2000 before we started legislating on ICT. Revised Penal Code, for example, on Article 355 on libel, you read that with Special Penal Laws, the E-commerce Act, the rules on electronic evidence of the Supreme Court in 2001 – that already gives you the framework penalty for online libel, which is an existing crime which we have already seen about 80 to 85% of our dockets in our cyber forensics laboratory already dealing with online libel.

We don't want that to be the priority because it has been catching up a lot of our resources. But we just wanna say since 2000, we already have libel in our statute books.

What happened? Fast forward? This is now the framework 2012. We found out that even if you add these two, there was a whole range of emerging technology, new social media, new forms that have been described, new forms you are familiar with, which have not been legislated upon. And this is now the third block. Question: If you add these three blocks, does it cover the whole range of criminal behavior? Probably not. There will always be new forms, new challenges, as long as human society is involved, we will always have different aspects to probe. But at least that gives us a fighting chance…

So welcome to 10175, the most controversial bill to date and the most social-media friendly. As we discuss the law, it'll be easier for you especially if you're reading the law for the first time. Okay. 10175. It's wired so you can download the site or whatever it needs to take.

Let me now go to the first section, libel. And this is now the default provision of 355. Two years ago, if a government official will present to you this line, which will actually be scandalous, of a baby saying these words, "*PUTANG INA MO*." This is something that we never hear of in a public forum, something that would be scandalous; in fact something that's totally out of character. But we'll not be hypocritical. You see this all the time and this is just the most benign form. A baby saying "*PI mo*." We're not even blocking the "P," blocking the "I," putting asterisk. That's just how it is. But the question now is, if this was put on your Facebook account? Is it actually libel? We have judicial rules for that. And this is not the forum to discuss whether what's libelous or not. That's not the whole point. But the question that we're saying is that with or without this, we are very sure that we are entitled to our online reputation. Correct? We already have a sense that I have a right to my reputation, a good reputation. You also have a right. And this is where it becomes tricky for media because now you're reporting it, now you're saying this but at the same time, you've also experienced it on your own. When you have been attacked personally, when your family has been attacked individually. This is something that is a dual-edged sword. And whether or not it's decriminalized, there's a flip side to it. Because it is a criminal behavior, the standard is proof beyond reasonable doubt, which is a high proof. Some people are saying you just go for a civil liability or fine. That's fine. The proof will be lower but easier to prove and probably more fines. So these are the debates that we need to have because you remember in 1932, when the Revised Penal Code libel provision was done, nobody was alive, or maybe one or two of two were already born already. But we never had the chance to participate in discussing

what is private to you, what is private to me? What is criminal behavior to you, what is criminal behavior to me? We never had this discussion in our history as a society, as a country.

That is why on a parallel effort, the Department of Justice, since last year, we have the writing the New Criminal Code of the twenty-first century. This one is something that I'd openly like to say, what is private, what is not; what is libelous, what is not; what is criminal, and what is not; so we can move forward. The small caveat that has also been raised is this portion, "other similar means which may be devised in the future." This raises the specter of A – What is the limit of libel? Wouldn't this put everyone into trouble? This provision. This is not something to fear. And aside from the three decks of slides, this also going to be a short language class, if you don't mind. In law, and this is for the lawyers, we have the *ejusdem generis* rule. Correct? For all the lawyers there or for legal speak. *Ejusdem generis* is Latin; it says "it's of the same kind;" and this is not from a law book, this is just from the Wikipedia. It says "if it's of the same nature as the enumerated, whatever follows should be of the same kind. So far, so good. What does that mean? "Through a computer system or any other similar means which may be devised in the future." This part talks about computer system. So this one can only qualify that it has to have the nature, characteristics of a computer system. Nothing beyond that, nothing out of the box. So you have to appreciate that in the context of the *ejusdem generis* rule, which any two-bit lawyer, any law student, will tell you it's something already existing. Okay.

This one, I would like to quickly introduce this and let me move over to this part of the stage. Section 1. "It shall be unlawful for any person, not being authorized by all parties to any private communication or spoken word, to tap any wire, cable or by using any other device…" all the way it talks about dictaphone, dictagraph, dictaphone, walkie-talkie or tape recorder or this is the italicized portion, "*however, otherwise described.*" This is the same *ejusdem generis* rule that has been protecting us since 1965 because of the Anti-Wire Tapping Law. Because we could not predict all the forms of media for so long as it forms under this particular description, the anti-wiretapping law extends the protection to your civil liberties. It's that something different? Not something strange? But the same *ejusdem generis* rule. So far, so good?

Okay. Section 5. Other offenses. I personally and professionally don't know why this is being questioned. Aiding or abetting, attempt, this is all over our statute books. In the Convention on Cybercrime, aiding, abetting, attempting is also a crime. This is equivalent to the frustrated, attempted stage. This is equivalent to the accomplice-accessory rule which we have in our statute books. Nothing strange with this.

In fact, one penalty degree lower, so nothing strange with this. We don't find anything particular difficult to explain on this particular aspect. That's Section 5. This is now the trio of Section 5, 6, 7 which was accommodated in the Bicam, 5, 6, 7.

Let's go to 6 now, I'm sorry. Can you read this? It says, all crimes defined and penalized by the Revised Penal Code…. This is the add-in provision, remember? Section 6?... That all crimes the Revised Penal Code, if you put it online is also a crime under the cybercrime law. This is what it is, and the one-degree-higher penalty that is already being questioned. I'd like to bring this into two parts. I'll discuss this in the next slide, and then I'll talk about this in the next slide. There's another language course. It says *expressio unius est exclusio alterius*. What does it mean? If I point to five of you, that excludes 95 of you. That's also a basic rule in law. So far so, good? Okay. The reason why this is in is because originally in our technical working DOJ draft, we never went into enumerating specific content acts. No libel, no cybersex. None of that. We just want it content-related, which is something that we aspire for as in International Conventions. But as we go along, people tried to put cyber defamation, cyber threats, kept enumerating, kept relating until we got to the point we said "If we keep on enumerating

all of this, it means that those that we did not enumerate under the Revised Penal Code or the Special Penal Laws is excluded from the Cybercrime Prevention Act." Correct? That is not true. There is no enumeration of cyberthreats, but you and I know that if I threaten you physically or if I threaten you through email or text, those are crimes. There's no question on that. Now if we don't have this provision, what happens? The defense lawyer will say *expressio unius*, it's not in the law therefore it's not punishable. That was the problem we faced when we're facing down to the last parts of the legislative proceeding. So we said, "You might live with this better, "lesser evil" so we can fix it in and explain in the IRR that this is what it means." Remember, Revised Penal Code plus Special Penal Laws plus Cybercrime Law. The whole point in the cybercrime legislation was just to legislate on the third block. But since Congress kept on picking out from the other blocks we had to say "Let's make a generic application so that there's no defense of say *expressio unius est exclusio alterius*. So far, so good? Okay. This revised one degree higher, don't be surprise, actually it starts with Section 4 but nobody's saying this. In child porn, it's only one degree higher. Okay. I will not beleaguer the point because we have differences in opinion and some people will say "two degrees higher," some people will say "death penalty," some people will say "decriminalize it." That's a legislative debate. Let the amendments take care of that. But this is not the first-time you're seeing it. I just want to make a quick correction. In all the fifteen (15) petitions, they were saying that the penalty for libel now is 12 years, 10 years. That's an incorrect appreciation of the law. Presently, its 6 months to 4 years. The correct reading is 4 years to 8 years. You may or may not agree with the penalty, I just want to correct an objective fact in the petitions. The fine is 600 to 2,000 pesos, that was 6,000 pesos. Not a lot of money but of course you have your own different interpretation which we will clarify in the IRR. So hopefully, that takes care of Sections 4, 5, and 6.

What's after Section 6 is this section: Liability under the Revised Penal Code and other laws… "Prosecution under this Act shall be without prejudice to any liability for violation of any provision of the Revised Penal Code or any other law." Question: What do you think of this? A lot of people are raising this section as a problem on double jeopardy. That you're punished online, you're also punished in the physical world. Anything wrong with this? Anyone? The basic question is this is not Section 7, it's Section 17. This is not a typographical error, ladies and gentlemen, but I refer you to this one, which is now where this comes from. This is Section 17 of RA 8484 of the Access Devices Regulation Act. It's been there since 1994. It's not the first time we're seeing Section 7 in the Cybercrime Prevention Act. It has always been in our statute books. We've been using it. There have been a lot of Supreme Court decisions that have talked about other liability. The basic double jeopardy rule… we will never change. The Department of Justice will be the first one to say "If double jeopardy, we will not do that." But if it is two separate acts are committed in two separate worlds, you would be liable for two separate crimes. If it's just one act punishable by two crimes, we have to pick which one is better, makes sense to prosecute. Okay. So this is Section 17. Look at Section 7 of the Cybercrime Prevention Act. I don't know if it's an act of faith, that 17 and 7, they're both 7, lucky number for us. But if you look at it, it's the same provision. Unless we're willing to invalidate all the other laws, we have it in the statute books, ever since. Does it change the double jeopardy rule? No. You know, for all the difficulties we have in government, nobody wants to keep on filing cases. And if you keep on filing cases as a matter of use, that's a different story. It's a human factor; not the legal factor; not a policy factor; definitely not a technical question. So far, so good with Section 7?

Okay. And I just want to cite quickly. We invited a couple of media personnel and I'm taking this quote from the blog of Raissa Robles who I held in high esteem for her investigative journal. But let me just illustrate Section 7 by this. She says in her blog "For instance, I told him, an interviewee, if a woman commits adultery using a computer, she would be guilty of a cybercrime and her penalty would be one degree higher." This is the question on the one degree higher. Correct? Second, "To use my previous example, I'm referring to this one, of the case of the woman accused of adultery, because of Section 6, if a married woman's email to her lover was submitted as evidence, the penalty becomes

one degree higher." Pause for a minute and with all due respect to Raissa, can you help me think of a scenario when adultery can be committed, with the, through the computer. I had a nightmare last night and said how can I answer this provision? In what instance can I commit adultery over a computer? Seriously, I can't think of any situation where adultery can be committed through… with a computer maybe but not through a computer. Okay. But the whole point is you have to be very careful of this, I mean as I said I respect Raissa and all of that. But the question is she might have been confusing the mode of proving adultery – electronic evidence, emails versus the fact of adultery. Two separate things. No two separate prosecutions, definitely no higher cyberadultery. No cyberadultery, definitely. I can say that. There is in law what we call the *factum probandum* and *factum probans*. For the lawyers here, two different things. Sounds like, looks similar, totally different. So with all due respect, let's be careful in blogging because when lay person reads it, it creates another chilling effect or whatever it's called. Let's have a seasoned debate, a very clear debate on what it's all about. So far, so good? Good.

Okay now, this is the favorite part of our law enforcement and the nightmare of our telcos. It says real-time collection of traffic data, the standard is due cause, does not require a warrant. Now, what is collection of traffic data? I'll refer you to the definition. Traffic data means non-content data. What are these forms? Traffic data refer to the data on the origin, destination, route, time, date, size, duration or type of underlying service. People would say you still need a warrant for traffic data. In conventions, laws of other countries, nobody requires a warrant for traffic data. The Department of Justice and all the way down to our field offices will never touch content-data without a court order that is administratively liable, criminally liable, and civilly liable on the part of law enforcement. Remind us, bring us to court. We will charge them report it to me if the NBI or the PNP is the first to open content without a court order. We're very clear on that. That's a line we do not cross. Okay. But on the traffic data, it's a different matter. Let me illustrate that. Traffic data is literally traffic along EDSA. It's not something that you not see, something that you experience everyday. And if you don't notice, here, we already have CCTVs anywhere. In fact, as I speak here there are already CCTVs. When you move through the Landbank building all the way here, public spaces, we are already monitored. For what? It's a public space, there's no claim to privacy. Okay. Now, when we spot a bus here, there's a plate number, or if the plate number is not there… if it's a fake plate number, what happens? You can record that. It is public space, it's public domain, especially if it's a kidnapping-in-progress or a terrorism target moving to the bomb destination. Nobody questions why this traffic data is being collected. Similarly, and this is the nearest parallelism, if you migrate traffic data literally, to the online world, how many emails are being sent? You don't know who, you don't know what the content of this email, subject to some technical niceties. But the basic idea remains, traffic data will not, should not, require a court warrant. Simply because, given our slow justice system, by the time we get the warrant which takes a couple of weeks, the data is gone. It's very volatile. It's very, very ephemeral. And the Supreme Court has said ephemeral electronic communication is an acceptable form of evidence. So that is the position but of course we will have safeguards along the way, which we will illustrate on the last part of the slide. Similarly, this is our post office…. When you register or when you login… When you register or will send letter through a post office, you would say the sender's name, "How much for the postage, from Manila to Tawi-tawi; from Manila to Hongkong?" Those are not private, there's no stifling of the right to privacy. Those are objective data that's verifiable, that does not infringe on your right to privacy based on content-data. Okay. That is the framework approach; we can read back on that.

Now, everyone's favorite part, Section 19. Let me clarify this. Since last week's interview, we have said, do not use the word take-down liberally. Talk to your technical friends, maybe Lito and Abet from PhCert, can discuss this clearly. Take-down, restricting, blocking are two different entities. Very, very separate. Take-down requires a whole team of forensic people going to the telcos and literally, physically taking down that particular data. That's almost impossible to do. Restricting, blocking, we will discuss

that in the next slide but the basic framework is it's not the take-down provision. Everybody says "take down, take down" even the Supreme Court says "take down, take down" but we need to exercise rigor because this is one slide that has a technical dimension because of the nature of cybercrime. Okay. So far let's leave it at that because the easiest way to understand Section 19… I'll give you a very quick tip just because here, you just have to move it three sections up. Instead Section 19, put it after Section 15, which is in the original formulation. Because, after adding it all in from Section 15, went down to Section 16, went down to 17, went down to 18, now it's Section 19, and when you read it seems very arbitrary, out of place. But the whole idea is not. In the IRR, we hope to arrange some of the provisions. Section 19 now, at least, will come after Section 15, protecting the law, no change but making sense as how it works. The original formulation talks about some kind of authority not the DOJ although there's a certain equivalency that I will explain in the last slide.

We have already initial discussions in Section 19 because as we said, our TWG version was cut up, we have to make some analysis. And when does this apply? I got this question many times last week. It will apply in very restricted cases. It should be case. It should be transcendent. There should be time critical element. It's not going to be just for any website there. The clear and present danger rule has to be met. There's a reason for us to go to restricting, blocking it. Commission of patently illegal acts; live-streaming of a child being raped, possibly. And, if you look at this, the Luneta incident, remember, the infamous Luneta incident? It disrupted this rescue and the safety of all the massacre victims, and somebody actually live-streaming all the data. Perhaps in that circumstance we would say restrict, don't do it yet, because lives are at stake. Very, very restrictive, very very close application of that.

How to make IED's? I don't know how you feel about this. If you think it is free speech or free information, that's fine. But in certain countries, how to make a bomb, how to assemble, the electronic detonation… those sites you can't access. Keyword: blocking. But we will not discuss that, it's gonna take a different narrative.

Another situation is creating panic or fear. Let's say, after this forum, a website says "All participants of the 2012 Cybercrime Forum contracted AIDS in the Landbank Plaza, 10th floor." Now, it's creating panic, everywhere you go everyone says "Stop, we don't wanna deal with you, you just came from the Cybercrime forum." Would that be a ground? A school infected with SARS-like virus, which was not true. Those are the specific circumstances that Section 19 could possibly be invoked creating panic or fear, terrorism. A live going on-stream and says "XYZ, we're going to bomb this."

Extortion, kidnapping? We have to discuss the contours of this because, as I said, the law has been arranged a bit; we need to rearrange it in the IRR to make sense of it. "Mass suicide, at six o'clock, October 9, we will have a common pact, let's all bleed to death against the Cybercrime Prevention Act." I don't know. For you to talk about.

Quarantine? The Department of Health says "Wait, nobody goes out this house yet; nobody comes into the country yet. You've been suspected of flu-like syndrome, hold till you prove you're okay or 'til we check the symptoms are okay." There's some shifting of the burden but not totally unacceptable.

Public health issue. Warrantless arrest, we're very familiar with warrantless arrest. We have very clear exceptions about seven to 10 in our statute books that say even without a court order, you can be arrested. And this one is the arrest of a person, a live body. In Section 19, we're talking about inanimate objects: a website, a page that causes terror, a page that causes massive suicide. That is a different parallelism. There's no immediate threat life or liberty.

And I was hoping that we would also have a very strong, vigilant type of monitoring, for checkpoint search. We see a lot of abuses in our checkpoints. No warrants required,

you're driving, you're stopped, you're searched. That is a bigger danger because at that point of engagement, at midnight, you're driving alone. Perhaps you can be a lady driver, or a young adult, that is where the real abuses will come in. It's because of the immediacy of the search or the arrest.

At present, the Department of Justice already does HDO's, watch-list, we also already arrest people. This is what we talk about the awesome powers. There's nothing more awesome than investigating you for a crime, NBI arresting you, or deporting aliens or stopping aliens from entering the country, who are yakuza members or triad members. There's nothing more powerful than those acts. Restricting, blocking access in the hierarchy of powers which the government has is very low. It's not something that is painted as awesome power to do this, it's not. In the hierarchy of rights, I've always said this: we'd rather have a department that is used to managing high levels of power, taking care of the abuses, knowing how to entrap people. You would want to give certain powers to that rather than just giving it to anyone who is not used to the notion of power and the responsible exercise of power. Wait until you're indicted for a criminal charge for murder, for *estafa*, for fraud. That is where you will feel the power. Not in restricting or blocking an inanimate website that has been adjudged prima facie to be illegal or meeting the clear and present danger rule.

Having said that, and because of the widespread concerns of this, what are the several things that we are looking at? One, the law talks about prima facie and we all know, this is another mixed slide, prima facie is a higher standard than probable cause. Right now, for a person to be charged in court the standard is probable cause. This standard requires prima facie which is a level higher. Which is the lesser evil? Probable cause for filing a case, or *prima facie* for restricting a bad website? I think it's very plain to see. It's easier for a case to be brought against you for murder, for a no bail offense for illegal recruitment, for qualified theft beyond two hundred thousand, rather than facing a restricting access order. So, I just wanna put that in context. But we also don't want it to be open-ended. It cannot be forever. We want to restrict our own authority and say "Perhaps I need a shell three days then we asses it, perhaps with academic civil society review people to see if there is there reason to restrict the data. If not, we take it off. That is the contour of what we're trying to do. *Ex parte*. People are saying court order but in the nature of cybercrime, where do you serve the processes? To whom do you send the subpoena or the summons? There is no person that we can reach for and by the time it gets there... that is the nature of cybercrime and *ex parte* is but part of the process. But as a measure of control, we will do a notification process and say "Doj.gov.ph has been restricted because of one, two, three. If you think this has been erroneously done, please contact ABC." And that will include the Commission on Human Rights, Office of the President, may be ITAP, PhCert, certain private sector organizations that can say "Hey, that should not be restricted". Three days, not three hours, three days consistent with Article 125 of the Revised Penal Code and a variant thereof. We also have a problem attribution. If you have a website like Globe, that says "I, Rudy Salalima is the owner of this." Attributable? We don't have to do anything more drastic. But a lot of websites that we see are based on dummy servers, IP addresses that are masked. We don't know anymore whose attribution it is, this particular website. How do you proceed against this? You send notices? It's a physical, technical impossibility. You cannot send all of this information to somewhere out there in the world and that is perhaps the reason why Congress deems it a good idea to have this stop gap measure to protect the community at large.

And the element of publication after notification, we will continuously update a list of public site that says this site has been restricted; all of these sites are child sex, selling Filipino children. All these sites selling fake drugs which will injure your health, possibly.

The contours, we don't know yet, it's an emerging field, and we all need to work together. And then we will also provide a process of appeal. Whether it through a

council or advisory council or through just posting it and say "hey can you help us with this particular website?" We will have an appeal process to make sure we will check our own authority. You know, in our saying, we always have a saying that we have good intention in a lot of things that we do, but the highway to hell is also paved with good intentions. We don't trust our good intentions. We need the private sector, we need civil society, and we need academe to watch government, to make sure that our good intentions are mixed with good methods for good results. We don't trust ourselves; we have good intentions. To do what is right, but we don't want to be complacent and trust ourselves just to do the right thing. We need you to watch us, we need it to look at us and say "Hey! That's out of bounce, stop." We need you there, eyes on the ball."

Finally, the last couple of slides, noncompliance, very easy. This is directed to telcos and ISP's. It's not directed to individuals. Because for the past ten years, this has been our frustration, ISP's routinely ignore the request from law enforcements simply because there was no enabling law, and even if there's an enabling law, there's no penalty. So what? My commercial business interest takes precedence over certain rights especially when the standard of trust for law enforcement is very low. When credibility of public institutions is very low, private institutions will ignore or try to circumvent or not try to comply with public sector orders. Very irrational behavior. So we will exercise this responsibly and again to a conservative process. In fact later, the announcement will be I'm pre-empting myself. Because of your presence here today, we would like to convert this forum into a collaborative forum of doing the IRR to see how we can move forward. We're developing a new model in cybercrime enforcement in the world. Let me repeat that: cybercrime enforcement in the world. Can you imagine all the hacktivism… all hacktivists for the two weeks and say "Okay, the next two weeks why don't we hack all the child-porn sites. Why don't we hack all the pedophilia sites? Why don't we hack XYZ sites that are bad for society?" Can you imagine unleashing the power of each individual using crowd-sourcing technology and then finally putting a stop or at least managing some of the bad problem instead of attacking of the government websites bringing down State resources? But I'm getting ahead of myself.

Is there more after the challenged sections? Yes. The final slides, are always about the question of we have too many laws. Yes. The problem has always been implementation and implementation. We always forget to ask what is implementation? We never had the component to say "Is this a good law, is this properly implemented?" It's always knee-jerk, it's always cut and paste legislation. For whatever it is, we're asked what the forum is all about. Hopefully, we will be able to advocate and say "Let's not have piece-meal legislation, let's not have a cut and paste legislation. Put everything together. It's not working for the past 60 years, maybe today with this law we are seeing the weaknesses of this particular type of legislative process.

But what is implementation? Let me say this. Implementation will take one, two, three, four, five, six. And this is not something new. This is from academic research. I just put it in plain language. But basically, whether you're a private sector, law school whatever it is, this is the formula to make implementation work: (1) Understand and assess needs. Talk to law enforcement, talk to the BPAP, talk to the IT expert, talk to everyone. What do we need for cybercrime, for cybersecurity? (2) After that, you develop a framework approach. What do we want? Freedom? Number six Internet freedom in the world or some form of responsibility? How do we do this? What are the contours of that? Open a public discussion list. That is the framework approach. (3) And I will comment on this quickly, hard work of course, ten years in the making. Let's leave it at that and I wish you could all acknowledge, and just give a round of applause to all the TWG members for the past ten years that had been with us in this fight. Can we just give a round of applause to all these guys for the past decade? We'll have a small panel later and you will see who are these guys who have stuck with this advocacy for the decade when I was still a young prosecutor. (4) And then structure, I'll talk about quickly about structure. And if you haven't read this, please read the statement of PhCert on their position on Cybercrime Prevention Act. One hundred percent (100%), we support the statement of

PhCert. (5) People, this is where you and I will come from. Good and bad laws, good and bad people, it's a very volatile mix. Good and bad people, sometimes it's a random act. Good president, bad president, we never know. But at least good laws, we can always aspire for as a body-politic. (6) Finally, a feedback loop and this is probably one of the reasons why we're having this forum so that from the feedback, you put this all together. This is how the implementation framework is.

And I would like to say that Sections 4, 5, 6, 7, 12, 19 and 20 are the least of our worries aside from implementation. Our real worries are as follows: (1) the first problem with this law is the confusion between cybercrime and cybersecurity and this was the time before Usec. Casambre. Usec. Casambre, this is not your fault ha. It confuses cybersecurity and cybercrime. The first time it mentions cybersecurity is in the definition. The second time it uses it is in the last. Those are the only mentions on cybersecurity. So my problem now as a legal IT professional is that we don't want legislator mixing cybercrime, cybersecurity. These are two different animals. Cybercrime is a penal legislation. Cybersecurity is an IT policy framework. When you go to a restaurant, what do you ask for? You ask for a menu. When you want to build a house, a dream house, you start with a blueprint. Here, it's a very confused blueprint, talks about cybersecurity and cybercrime. We have consistently said: just put this in cybercrime, the cybersecurity, DICT to follow. Remember that three-pronged strategy we have in the beginning, let's not confuse the three. But apparently, the message did not through, we have this confused mindset. And confused mindset, leads to policy implementation challenges. Solvable? Yes. A bit more challenging? Yes. More difficult? Yes. More sleepless nights? Yes. Easily preventable? Just make an amendment: cybersecurity, cybercrime totally different animal. The other problem we have is cyber-squatting. Nobody has mentioned this. But cyber-squatting is misplaced in Section 4. Cyber-squatting is not part of the Section 4 concept. It was just placed there and now in the IRR, we have additional work to find out how cyber-squatting can fit mindset. Because you and I know, whatever you do, it starts with the mind. You understand it, you comprehend it, you rationalize it then you move forward with the action steps. Here, the legislators give us a piece which we're responsible. We're holding this forum, spending time and effort doing this, but cyber-squatting. How do we manage this? This is a totally different thing that we don't want because it confuses the law and at the same sense it mixes cybersecurity and cybercrime, but it's there. We'll do what we can.

This, especially I'm addressing this to women advocates and children advocates. Be very careful with this, work together with us because in Section 4(c)(1), it punishes cybersex. Remember this era of hauling women from cybersex den, being photographed and their hiding their photos like this. Remember? We thought from the Department as child and human rights advocacy that this was a thing of the past. If there's something medieval about the law, it's this particular section. Why is that? Because when this was legislated like this, it did not consider all the other provisions. Therefore, based on the reading of that particular cybersex provisions, the concept of cybersex or trafficked women as victims is now fudged. We need to fix that in the IRR to clarify that women victims who are exploited, who do it out of economic necessity, who may not be as privileged as you or me, will not be punished of the era where they're hold-off to the NBI or PNP, taken photographs. That is not what cybercrime prevention act is for. It's against the criminals out there, transnational organized crimes out there that are destroying the fabric of society, not against women and children like this. So help us, if you have women's group; women's contacts, let's start looking at how the IRR can harmonize provisions of this and yet maintain the spirit and point of the law.

And this brings us back to my final point, about all of this laws being passed piece-meal. There's no framework; there's no aspect. Hayden Kho, let's do this; many child pornography issues, let's do this; trafficking issues, the USS, human trafficking, let's pass this. E-Commerce Act, I love u virus. Access devices, strong lobby from credit cards in the banking industry. Crime Prevention Act, who knows? We need a framework of how we want to punish criminal actions in our country. And hopefully, this will be a

start of a new beginning, let's this be a lesson learned for everyone, you cannot legislate without the context in a vacuum. And that's creating a lot of problems. When law enforcement goes against the bad people, we're confused with sections to use, some sections are conflicting. You would file Section 1 RA 1 in relation to Section 2 RA 2, in relation to Section 3 RA 3. Makes for bad law, makes fugitives, and makes it funny for law enforcement in the Philippines.

Last slide and this has to do with the implementation issue. This is now the web decision that we have, are you guys familiar on how the web structures works? Correct? It's distributed, there's no single central node, it's meant to be just available anywhere, everywhere. So far, so good? Even the neck tech people will understand this. This is now the model, but when legislators were legislating this, they have this in mind: a table of organization to implement the Cybercrime Prevention Act. We have been very consistent and say if this the model, if you want to design a structure effectively for implementation, then your model for implementation should at least mirror this. Because you're after a certain specter, you're after a certain phenomenon. So you need to design it carefully so you can be responsive and flexible and dynamic to meet the threat of cybercrime. But apparently, this is what they have in mind as legislator. Table of organizations, and then by the time you get a quorum, you don't even have to worry about getting a court order. And we've been very strongly against it and again this is before time of Usec. Casambre, the CICC, we have to tweak that a bit because just getting a quorum, the enforcement is already gone. So we also have to fix that maybe through operation center to make sure that we are nimble enough when there's a kidnapping-in-progress, when money is being transferred out the country, for money-laundering reasons or there's a drug syndicate that's about to do a buy-bust operation. Those are the things that we need, not blogging, not tweeting, not liking.

So, last two slides. That is now the criminal justice response. These are the things that we've lined up. This is a product of ten years of work. We now have a Q and A guide on cybercrime. This will be available for everyone maybe in different languages.

The Joint investigation manual for Law Enforcement and Prosecutors, we also want to delineate PNP and NBI, so we don't have duplicity in resources. We already have 150 trained investigators courtesy of Prosecutor Arellano. Electronic Evidence Guide, this is now manualized, to guide everyone even private sector on how to use electronic evidence. This is about 100 pages long but very easy to read. But what's the beauty of this, you just have to have to use the forms. What are the forms for complaining? What's the checklist for chain of custody? What's the checklist for going to courts? This is the effective way to interdict transnational organized crime. These are all in various stages of preparation because we have to wait for the law and of course the petitions. Regardless of the outcome, we will of course work with what we have.

Accession to the Convention on Cybercrime. I'm very happy to report that we have been invited to accede to the only convention on cybercrime worldwide and hopefully we'll be the first developing country to accede to this, in due time. We have to do this in less than a year, and we will be COE compliant. Just a short story, once when, when we got the enrolled bill at the last minute, we were not getting a copy of the last portion. We immediately sent it to our Council of our Europe counterpart and said that "This is now the present cybercrime bill. Will it meet the standards of the Budapest Convention? Please do a quick review." Because if it doesn't then we will have to recommend we change it because what's the point of having a stand-alone cybercrime law. You need to work together especially the server are in the States, the servers are in Singapore, the servers could be anywhere. It has to be international cooperation. Their answer was yes. It's 80-85% compliant. We have certain reservations but if you pass this law as it is, you'll make the cut. So, we recommended it to the President "Sir, let's go for it, better than nothing. Lets' just work on the implementing rules on how we can make it better." So there's full visibility at least under executive going up. That's our recommendation. What could have been the other part? We recommend, "Sir, we have problem with the

structure, cybersecurity cybercrime is confused, libel should not be there, all of these little things should not be there." What happens? We go back, another Congress, we don't know. So we said, "Let's go ahead, and see how we can work it out."

Network of monitors and investigators, this is where you come in. Ah, your favorite part. We are trying to build up from the law how the procedure goes. From the time you complain, from the time you feel offended until the time that you get to report it. So this will be consulted. We will not use the traditional model in the investigation because that's no longer relevant. We will see how that goes.

And speaking of this, we need a societal response that's why we're saying the Philippines will lead the way in criminal law enforcement. Internet safety for children. We are very young population. Very internet savvy. Very, very high internet usage. We need our own protocols for Filipino children especially if they are in single-parent households. Very unique in the country.

Civility in cyberspace, the golden rule in cyberspace, very simple. *Huwag niyong patulan yung nag-aaway sa* Internet. *Hayaan na lang natin*. We don't have to have this speculation. Last night on primetime people were saying, the DOJ has a dubious agenda in setting the forum; the DOJ has a dubious agenda in moving it to Landbank; the DOJ is trying to coop all the critics. People can say anything, say everything, but the best is always to appeal to higher sense of intellectual discourse of reasonable discussion among Filipinos.

Restorative justice, I'll skip this. We'll get back to that.

Crowd-sourcing as I told you, we want to have a process there maybe the ten (10) major ICT companies or ICT groups can say, "We received this complaint. We have verified the particular complaint. It's not a harassment, it's not something;" and maybe have an express lane. We don't know the contours yet, as I said we're developing a new strategy to fight cybercrime. So if the ITAP or PhCert says, "We have seen this complaint, we have done this, and we know this person." Then it goes to express lane, so to speak. So that saves as a lot of trouble. Remember, government cannot do this alone. The beast is so huge; we have to do it as a collective.

Accreditation. That's what I was talking about. This is a bit; this is the last slide now. I'm both happy and sad to show this to you. This is the first complaint that we are docketing under the DOJ Office of Cybercrime. And we saw this on the eve of October 02, and we received it on October 03. This is the first child-sex porn complaint that we have. And it's happy because it sees the trust in the Department, in government in general. Sad because while we were blocking out the private data in this, we felt very stupid doing it. Because this girl, this 17-year old Filipina who was first abused when she was 15, her identity is not secret. Her videos are all over the internet. The permanence is there and she's crying for help and saying what the government can do for her. She can no longer face her fears; she can no longer face anyone. This is a cry for help that we're trying to respond to. What can we do? Can we really stop all the videos? No. The least we can do is to provide restorative justice, provide counseling for a woman, maybe relocation, and different identity. This woman is gone. Her reputation because of the online scandal video, the immaturity of her age. When I got this 2 days ago from Secretary, it somehow validated all the 10 years of work – of all the frustrations with legislation, all the difficulties with all the critics from left and right – and say this validates that, for so long as there's one woman, one Filipino, one vulnerable person there who can step forward and say "Ma'am, Sir, can you help us with my particular concern?" It's worth the effort. It's worth the fight.

So lastly, these are the three things. We will convert now with your permission: collaboration with all stakeholders to make this a truly collaborative effort. IRR… bombard us with the position papers. We'll open the websites for comments, questions…

Engage, engage with us. As we said this is the first cybercrime forum, it's live via web stream, it's globally available, and all our sites are ready. Just knock, we're here to listen. Second, I'm very particular on oversight on law enforcement agencies. Who polices the policeman? Who polices the media? Who reports on media? This is the most crucial task. The other issues in Section 4, 5, 6, 7, 8, 19 and 20, are not a problem. Overtime, it's a problem of cat and mouse issue. Weak justice institutions, weak integrity, law enforcement as the first violators of the law. That is where monitoring, activism, social consciousness and vigilance should be in place. So that's why we'll set up a procedure: before the NBI and PNP start reading anyone, start arresting anyone, start seizing anyone, clear protocols have to be addressed with clear conduct of that. Three strikes of complaints, you're out. That should be the standard of a cybercrime unit in the Philippines anywhere in the world because precisely of the nature difficulty of cybercrime. Make no mistake about it, this is the real challenge. Oversight and law enforcement agencies including the Office of Cybercrime. Watch us; watch our back; watch how we perform. If you're not happy, raise a petition to the Supreme Court. It's not gonna be too late. But I'll tell you guys October 09, 2012, this is the crux of the way forward. This is the whole point of the challenge of implementation of the law and in the Philippines. Last night, we wanna shift already; focus on syndicates and organized crime. Remember, this law was meant to target the most pernicious forms of crime, not bloggers, not critical citizen. Everybody can handle that. So with that, I hope I have not taken too much of your time, I intend it to keep it as small as possible, and thank you and God bless you all.

Emcee: Thank you Assistant Secretary Geronimo Sy. Before we pause for a break, we'd like to inform you that aside from the complaints and haters you also have someone tweeting about you being cute online. So that's good news. Okay. We'll have ten-minute break and then when we get back, after you help yourselves to coffee and some bread over there, we'll go to the open forum and we'll see you in a bit. Thank you.

Okay may we request everyone to settle down? We'll be starting in two minutes.

Okay. Ladies and gentlemen, for our open forum, I would like to call on our panelists who will entertain your questions. Okay. May we call on, of course, Assistant Secretary Geronimo Sy, Sir Dondi Mapa, Atty. JJ Disini, Congressman Tinga, Undersecretary Casambre, Mr. Rodolfo Salalima, Mr. Joey Narciso, Mr. Ray Roxas-Chua, and Ms. Bettina Quimson? I'd also like to introduce our moderator for this session; our moderator is the President of the Philippine Chapter of the Internet Society or ISOC and former SVT, Advocacies of the Internet Commerce Society. He is also a columnist for China Business Philippines and former editor of PC Magazine Philippines. Our moderator for this morning, Sir Winthrop Yu. Hi sir, good morning. Undersecretary Casambre? Atty. JJ Disini. Yes. Sir Rudy Salalima, may we call you to be part of the panelists please. Ms. Janet Toral, may we also call you.

Moderator (Mr. Yu): To Medias de Rivera and Lito Averia. *Dalawa kami ni* Lito *nakapula*. We're celebrating the cybercrime law. Okay. Good morning ladies and gentlemen. We open the floor to questions.

Ok. Good morning ladies and gentlemen. We open the floor to questions.

Question (Roy Ibay): Good morning. I'm Roy Ibay from SMART-PLDT and SUN and I'd like to raise a question regarding Section 12 which was discussed earlier and actually, I like to touch on the merits of its constitutionality or unconstitutionality vis-à-vis the constitutional provision on privacy of communications. We're just curious, the section actually states that the law enforcement agent, acting on due cause, may record the… monitor the traffic data real-time, so we're just curious if our bill contains the definition of due cause. Because I don't think there is a definition in the RA itself and…

Moderator (Mr. Yu): Yes. I think Asec Sy can reply to the definition of due cause. How.

Answer (Asec. Sy): Yes. It will contain the definition of standard due cause. And the basic idea is beyond mere suspicion. But there has to be a reasonable basis for doing so. That is the generic understanding of due cause as applied to section 12. But it's very, very clear that it will be in the IRR.

Question (Roy Ibay): Who will determine the due cause? Will it be the DOJ or…

Answer (Asec. Sy): There's an initial determination. We have not, that's why we're going to consult it first considering the immediacy requirement and given the contours of cybercrime. But initial determination will have to come from the Executive which is either a DOJ composite team, operation center or a composite team including the NBI-PNP but with oversight from the civil society. That is the direction.

Question (Roy Ibay): My last question would be, we all know that service providers like a Globe, PLDT, Smart and Sun, provide the transport or the highway for a lot of data and communication to take place and we are also aware that similar to US and European counterparts of the cybercrime and other related laws, there are certain qualified immunity provisions given to service providers and we're just wondering if the IRR would also give such qualified immunity provisions to service providers given that the premise is that service providers really provide the transport for all of these data and the communication to take place.

Answer (Asec. Sy): Very good. You don't need to wonder, there will be very clear safe harbor provision for telcos and ISPs acting in good faith.

Moderator (Mr. Yu): Undersecretary Casambre. Yes while, aside from the safe-harbor provision, probably one question is who will actually be implementing this …In the United States for example, if the FBI has an order to monitor or block, its an FBI agent that actually does it. Will this be the case here in the Philippines? An NBI agent will have to actually walk into a telco ISP or will this be simply an e-mail or an order from the DOJ to the ISP or telco?

Answer (Asec Sy): Si Usec. Casambre. Can we just give him round of applause for the great work? He has to leave for an urgent, pressing appointment but he assures you that he's with us online. So just remove the chair so… thank you. Who will be responding to that, somebody wants to…I wanna share the mike please, Joey? Can you?

Answer (Mr. Narciso): As I see it Sir, it would be best if an NBI agent will be assigned *dun sa mga* telco *natin* to monitor.

Moderator (Mr. Yu): Further questions?

Question (Chat Garcia-Ramalo): Hi. My name is Chat Garcia-Ramalo. I work for the Association for Progressive Communications. One of the things that you said earlier is that, your example around adultery and how that can be done through the computer. But in fact the definition that you have that the law has in the Cybercrime Prevention Act exactly says that, the definition says, and I'll read it to you. Cybersex – the willful engagement, maintenance, control, or operation, directly indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system, for favor or consideration. One of the problems of that Act is that defines it quite vaguely so under this definition, what is the limitation of cybersex? In fact, I think that is exactly the question you were asking. I'm not sure how then do you look at this? How do you make of this definition clearer when you're talking about implementing rules and regulations? One the things that we discussed in the form last Friday is exactly why cybersex, as one of the offenses, should be struck out of the Act itself.

Moderator (Mr. Yu): Okay. So the question is the making the cybersex provision less vague? Ahh yes..

Answer (Atty. Disini): Ahh actually ahh. Senator Guingona has a problem with that particular section. In fact his attack is on the meaning of the word, I think lascivious because he says that there is no stable definition for what is meant by lascivious meaning it's a..I guess a question of taste. Therefore renders that particular provision vague. The limitations, if any, would be in the phrase, favor or consideration. Consideration means money, changes hands and exchange for the exhibition of the lascivious content using ICT. The question in my mind is what is meant by favor because you could argue, all sex is favor. So in other words, it's all, that's a problem. Favor means, there's no consideration, how do you prove it? It's an exchange for something else. I think the other problem is that there is the word indirectly. So if you commit it directly, it's clear. If you are the one doing the exhibition then you are the one violating the law. Meaning the person paying isn't penalized because he is not the one actually doing the exhibition. But if it says but if it include indirectly violation, does that mean that he is also included? I think indirect was included in order to penalize those persons who engaged this as a business. In other words, they recruit women and engage in a business. But to me, its seems a little vague to use the word indirect in that. I think Congress could have been specific that one who engages in this as a business, recruiting others to engage in this type of activity should be separately penalized.

Answer (Atty. Salalima): I too, have a problem with that definition of cybersex. In fact, one of the constitutional issues against the cybercrime law is about the fact that some, *hindi naman natin nilalahat*, some of the serious provisions of the law are overly or vaguely stated. Now, if a punitive law is overly and vaguely stated, that law or that provision of law can be stricken out as void for vagueness. It is void for vagueness and therefore it is unconstitutional because when a law is void or is vague, you are not according the party who may later on be charged of a crime with due process. Due process presupposes that a party knows the law and knowing the law means that the party clearly understands the law because the law is clear. Now, there are a lot of provisions in the cybercrime law where even the definitions are vague they are overly broad and on the cybersex definition, the word precisely fares for favor of consideration. It would have been much better if Congress said for commerce because while the word for favor or consideration may have its good side, it may have its bad side. *Yung ngang sa* deed of sale *natin*, you cannot sell your property by saying for and in consideration of my love to my daughter and the additional amount of One Hundred Pesos (Php100). I am selling my lot to her. There is nothing illegal in effect as far as favor is concerned but in this case, we are using favor or consideration in a criminal sense wherein that word or phrase can be interpreted in a lot of ways. So therefore, because the law is ague, overly broad, it in fact exercises a prior mental restraint on the citizen because he is at a loss as to whether his act or conduct is criminal or otherwise. Unlike where a crime is clear, in this case, he can do anything for as long as he avoids the law because the law is clear. These are some of my statements on the law itself.

Moderator (Mr. Yu): Okay. One of the...still on the content... I believe Asec. Sy already mentioned that strictly speaking cybercrime legislation does not contain content-related provisions. Another question sent in online, regarding content is how do you intend to pursue and prosecute spammers? The sub-question is what about spammers abroad?

Answer (Atty. Disini): Actually, the provision on spamming in the law is quite broad. In other words *malaki yung* out if you're engaging in unsolicited commercial communication. The law does not require you're to have a pre-existing relationship with the person to whom you are sending the email, not with the exact person. You can buy that person's information right his email address from whoever selling information and then you can send it but there's requirement, there's an octal provision where you can

identify yourself. Now, actually what people don't understand is that there is a lot of overlap between this law, the 10175 and the data privacy law which is the 10173. Both laws lobbied, signed close together, and lobbied as I understand by the business processing association. People haven't understood yet the exact impact of the data privacy law but I can tell you like the example given earlier about saying releasing information about the health of everyone in the DOJ forum has AIDS. That would be a punishable act under the data privacy law because that's sensitive personal information about the health of individuals and that would be punishable under that law, and that's the problem and going to the problem with Section 6 and 7. It would also be also punishable under the cybercrime law if you do it via tweeting. And going to the double jeopardy provision, I understand the section 17, we just pointed out earlier which is similar to section 7, almost exactly worded. That is true. There have been other statutes such as BP 22 where it says that prosecution under BP 22 is without prejudice to prosecution under the Revised Penal Code. But in those cases, those are two different acts. The act of *estafa* has the… included there is intend to defraud, whereas in bouncing checks there's none. It's the issuance of a bad check. So these are two different crimes. But under the cybercrime law, which I think is covered by the double jeopardy, it's exactly the same crime. And your being punished twice because under section, under the Revised Penal Code you're punished and also, under the cybercrime act but one degree higher. I just like to mention one more thing about that this is a content-neutral statute. It is not. Because Section 6 incorporates not just the Revised Penal Code but all other criminal statutes existing in the books. The Cybercrime Prevention Act isn't just about cybercrimes, it's about all crimes. Any crime you can think of. Violation of intellectual property right is covered by the cybercrime law and intellectual property right is certainly content right. In fact even economic laws are included. For example, I think it's a crime to sell, to engage in retail trade if you're not a 100% Filipino. Under Section 19 on a prima facie finding that you're violating the law, your site may be blocked. Well does that mean that the Secretary of Justice can block a site like say eBay or site like amazon.com which is engaging in retail trading in this country is not 100% Filipino-owned? These are the questions. These provisions, independently of each other, may be okay but when you interrelate them, and when you interrelate them into to a larger scope because it's so broad, and under Section 6 of the law basically gobbles up all other laws. When you connect all of these dots, it's pretty scary, the kind of power under Section 19. So it's not just libel, it's not just content, it's economic activities. I think that would fall under the jurisdiction of the DOJ under Section 19 or the take-down provision.

Moderator (Mr. Yu): Thank you Atty. JJ. Further questions?

Answer (Audience): I just like to answer question with regards to the how to prosecute spammers or phishers when they attackers are nebulous. One way of doing it is to follow the money. Since December last year, there are multiple cases of phishing. Real money has been transferred in hundreds of thousands-----follow the money, they got the person and they are going to charge that person, their lawyers are working on with this new cybercrime law but that's how you attack the phishers, and the spammers, and the scammers. Follow the money and there would be a corresponding decrease in phishing attacks against your organization.

Moderator (Mr. Yu): Thank you Direc. So you follow the money in other words you've been doing this even before the cybercrime act was enacted. Okay. Thank you. Maam?

Question (Comm. Quisumbing): *Magandang tanghali sa inyong lahat*. I'm Commissioner Coco Quisumbing from the Commission on Human Rights. Just a warning in terms of that case, please try not to violate the rights of those people and make and apply the law ex post facto. We at the CHR understand very difficult and delicate balance between fighting and preventing crime but also protecting, respecting and promoting human rights. And while yes there is a need, definitely, there is a human

rights aspect in terms of fighting some cybercrimes especially the attacks on women and children, so thank you for putting that in. But we really need to highlight that the Philippines has obligations in our constitution and in international law – in treaties. *Hindi pinaka-importante itong* cybersecurity, the covenant on cybercrime. The Philippines has since the time after the People Power Revolution, been a state party to international human rights treaties that protect fundamental freedoms like freedom of expression and right to be safe in our personal correspondence and other effects. So there's that balance. We know that there are already court cases, complaints about especially the libel provision. But I just want to warn, highlight if we can work on that in the IRR, please let's do that. It would have been so much better if this was discussed very thoroughly in the making of the law because *alam niyo naman dagdag yan sa trabaho namin* with our budget getting cuts every year for the past three years. This is just one more area where we will probably be getting complaints. The Philippines had already been told by the UN Treaty Body on Civil and Political rights, that the existing RPC on libel is not consistent with our obligations. It says imprisoning people for libel and defamation is never appropriate. So the fact that we even included it in a new law; the fact that we increased is not a, it's not a step forward, especially because we have the obligation to create and maintain a legal framework, a legal environment where our rights can be fully enjoyed and even to promote. So we're hoping for some improvements in this. Definitely we look forward to the steps as Asec. Sy had mentioned in guarding the people who are supposed to be implementing it. But we also promise that the CHR will be active in formatting, formulating any such IRR but we will also be watching. Thank you.

Moderator (Mr. Yu): Thank you Commissioner. By the way, we have some people from the Information Communications Technology office here. Commissioner, I believe there was an initiative by the workshop or meeting has actually been called but I believe they were planning to draft something like an Internet Bill of Rights, and yes, Carlo.

Question (Carlo Ople): Hi I'm Carlo. I work for a TV network. I'm here mostly as a blogger. So, not a lawyer. So some of the legal speak gets lost on me. So I'll try to be very… *kumbaga* layman's term. Hello. *Ayan*. Okay. First, one quick comment, I think Asec. Sy if you were explaining this from the very start, *yung* time *na ina*-announce yung bill, that probably won't be as bad. So thank you for going through the lengths of explaining everything, how that you just did. I think of PR this bill was single-handedly destroyed by one senator but hindi ko na *babanggatin kung sino siya*. But anyways, I'll be very categorical and again I'm a blogger now so and I hope to get straight categorical answers. *Kasi marami ring* bloggers *nagtu*-tweet, *nagtatanong*. *Since wala masyadong* blogger so I guess I have to ask the questions. So for example in 2013, *may isang kandidato tapos* bloggers start writing about him in not so nice ways. Trying, pointing out some of the things that we disagree with, other stance, people reacting to what they say and they write it…. *sabihin natin* harsh way in their sites. Usually *naman hindi pinapansin* unless *naging* viral *eh*…but in this day and age when it's so easy for people to share, *sasabihin natin umabot sa* 15,000, 20,000 shares and suddenly plus a million views. Will that senator or that congressman or that politician *sabihin natin* have the… can that person can file a libel suit against that particular blogger or social media user? So I guess that's the first question. I have several if it's okay.

Answer (Asec. Sy): The straight answer is even if it is the harshest comment hitting a hundred million page views, the Department of Justice will not tolerate a candidate filing a libel case against a blogger of any kind or any nature. That's the straight answer.

Question (Carlo Ople): Thank you for that, *marami pong mga, maraming matutuwa*. Next question is *sabihin natin* on a similar line, there are industries that get a lot of complaints especially airlines, even telcos, *sabihin natin* some bloggers, writers, social media users air out complaints again in the harshest way possible, will they be liable for libel?

Answer (Asec Sy): I think you're setting me up for a trap. But again the straight answer is usually when we have the law then we have the implementing rules and regulations. What we have not done as a community is that after the IRR, we just leave it as it is. With this new law, with this new office, with the new IRR, after the IRR, we'll come up with guidelines. Guidelines on internet safety for children, guidelines for bloggers. What is the harshest critique you can give without being libelous? What are the signposts, what are the listening posts? That's why we can educate and increase the level of academic discourse and not talk about showbiz all the time. So I think that's one area that we can work together on. Guidelines that will help you and I clarify what are the limits of free speech because free speech is of course not absolute.

Answer (Atty. Disini): Yeah…umm…so I understand that the Department of Justice will say that they will not file that case against you for libel if a politician were to file it against you. The fact of the matter is that recent history has shown us that these politicians do file libel cases. So if you're blogger, you're just at home and you're blogging on your internet connection, if somebody sends you an e-mail, says that's libelous and he is going to file a case against you. In order for you to say "That's not libelous because I'm protected by Mirror Times vs. Sullivan which is a US Supreme Court case protects your right to criticize public figures. Before you can raise that defense you would have been charged either in the city prosecutor's office or in court, of course, in court. In some of these cases, some of these cases go all the way to the Supreme Court. Do you have the resources to defend yourself up to that point? The fact of the matter is that whether or not that case will or should be filed by the DOJ is not that relevant because the fact that the matter is that you will not. You will take down the content because you are too afraid of what will happen to you. And this is why I think it's important in why the UN insists that libel should be decriminalized. Because it's too hard to know, in fact earlier there was that page that was put up with the PI of the baby and the question was that libelous? And I can tell you, I don't know. It's difficult to know what's libelous and what's not. And when the law is unclear, especially when there's criminal sanctions involved, there's potential for abuse and we've seen that. So I think that if we believe in free speech, if you believe that the cornerstone of any democracy is a marketplace of ideas where everyone is free to speak his mind on any public issue, then I think decriminalizing libel is the only way to go.

Question (Carlo Ople): I agree. Two more questions. Are publishers liable for comments left on their site? *Sabihin natin* it's a libelous comment.

Answer (Cong. Tinga): Can I just add something to this *lang*. I think it will address a lot of these concerns you have. I think the one thing that's coming out of all these and hopefully this happens in the future is you're going to see a change in how legislation is drafted. This will be the start of that. We came from… I'm happy to report this because I just came from a forum on E-parliaments. And we saw how in certain countries, legislation was actually being crowd-sourced. *Ilalabas mo yung* legislation *diyan*, people will put in their own comments. So it was not just blank criticism, you had to be constructive and productive. You don't like this portion, *tanggalin mo, palitan mo, ayusin mo*. Now, I think this is where we're going to have to head. We've been…me and the people who are involved in ICT have been saying this is where it has to go. I'm not a lawyer and you know…my parents are lawyers, but I think it's a good thing I'm not a lawyer. Sorry to the lawyer ha. Because with this, *mawawalan ng trabaho yung* lobbyist. *Ganun ang mangyayari dito*. And from the systems we've seen, you could see that if parliamentarians, MP's were not involved in listening to the comments and the suggestions of their constituents… Directly related *yung* grade *nila at saka yung* popularity *nila*. It was all online. So *hindi ka mag*-interact *sa mga* constituents *mo at anong sinasabi nila, nakikita yung* grade *mo*. It was that black and white. And I think that's the kind of people representation we've all looking for. So hopefully this whole exercise has shown us just how poor our legislative process is, including where I'm sitting. You're complaining about one bill. Dahil you're complaining about this anti-cybercrime bill and I can tell you being in Congress, being in government, there's a ton

of bad bills out there but you haven't have a chance to look at them. So I think beyond this you guys have to take the challenge to a bigger forum. Yes you're critiquing a bill and some of its components. We have to create the system for you guys to actually look at all the legislation that we are passing. *At hindi yung pag nailabas na at saka naghahabulan*. We're chasing after the fact here but I think this is an excellent forum for us to expose and discuss a bad practice *na nakasanayan na nating lahat*. This is my first and last term in Congress. I can say this, I'm not running for public office. But it's a problem of the system. It's not a problem of the individual. *Magalit man kayo sa akin, magalit man kayo dun sa senador,* the system is the problem. So I think here you guys have brought out something that the lawyers and the legislators can't fix on their own. I think it's something that because of this forum, we now have a chance to address.

Answer (Atty. Salalima): I am glad that the congressman from Taguig had expressed the intent of the Congress to review possibly amend them the existing cybercrime prevention law for the better. But right now, we are assured by the DOJ that they will pass an IRR which somehow would soften the law which is otherwise broad and vague. I know the person. He is a good-natured person. He always acts in good faith as far as I'm concerned, as far as my dealings with him are concerned. But my unease is reflected by the fact that the more Asec. Sy explains the law, the more I am convinced that indeed the law is overly broad and vague. Here lies therefore the defect of some of the provisions of the law. Now, we rely ourselves on the faith of this man, on the face of alleged impending IRR. The problem here is when you issue an IRR, clarifying the law to the extent that in so clarifying you may modify, you may restrict or you might over-expand the law, then that the IRR is void. Because in effect, you are supplanting the wisdom of the legislature by the wisdom of the DOJ, which you cannot do in legislation. An instance precisely where an IRR was struck down because it modified and in fact expanded the law is… remember that 13th month pay in our Labor Code? There was an attempt by the Department of Labor to put up an implementing rules and regulations defining anew the concept of 13th month pay. In that case of Chinabank, the Supreme Court said "No, you cannot put in the IRR something which is not found in the law." So how I wish the clarificatory explanations of Asec. Sy was found in the law itself or in the least, at least those clarifications were found in the deliberations of the law. So that at least, if the law is vague. We can have resort to interpreting the law on the bases of the interpretations in discussions of the law in Congress not in the IRR. Because the IRR in the law are meant to be implemented not only by the present government. It is to be implemented by future governments, and if Mr. Sy is no longer around, what guarantee is there for us to say that a very zealous prosecutor would say that IRR is a restriction of the law which is broad and therefore that IRR does not bind me. These are my thoughts on the law.

Answer (Ms. Toral): I would put a hopeful voice. *Kinakabahan ako sayo*. First, I think also for the CHR. I think that's something that has to be considered once the IRR is being drafted is what is our take on being anonymous? I know that we always want libel to be decriminalized because want to be at par, or we wanna be fair and be at par with other countries but we also know that libel has been, libel online, has been a great field for those who would like to take on anonymous identities and really struck down on persons online. Whether there was truth or not to what is being claimed but that is a problem and I think the cybercrime law has an opportunity to address that issue and I think we have to take a clear stand on that. Is libel decriminalized for known identities or are you going to apply the same to anonymous identities. Like for instance, I always mention about this site that was put up a list of men with AIDS and it was built by someone with an anonymous identity. It violated their human rights. But this person who put up the site was saying that people should know that they have AIDS because they can harm people. So I want to… maybe later on, once we start working on the IRR, I wanna understand what's your take on anonymity and on application to other laws, on IRR, the way I understand… Atty. Sy explained it earlier on how the IRR will be drafted, is that it will take into conjunction all other legislation where cybersex and pornography were tackled, therefore in the IRR, the way that will be explained is that not by this

Section alone, but it will also take into consideration, other laws and how they will be handled together. We experienced the same predicament with the E-commerce law because E-commerce law provided electronic document recognition for all the other laws. So that is why when they were trying to amend the IP Code to specifically mention electronic counterparts, what was being suggested then was to issue another IRR on how that law can be applied in conjunction with the E-commerce law. So that… define to further clarify it. So I guess, that's why I'm saying I'm hopeful that in the attempt to clarify not just to only look at the law by itself, but how the law can be applied into… with other laws to ensure that it will not conflict with other laws but more of supplementing the other laws, if that would be indeed possible. And I guess by the time we start doing the *bakbakan* on the IRR, we are gonna see all of that. So I hope we give it a chance.

Answer (Ms. Quimson): Basically, I'm from the outsourcing industry and I would like to state that to a greater percentage and we're very thankful that this law has been passed. As all of us, we have problems in certain portions of that law, specifically on libel and how that affects people using your premises and making you liable for whatever your subordinate or your employee is doing, at a higher level. Now, we were told that this would be handled in the IRRs and from what has been said again right now, I think guidelines will be the basis by which we really have to monitor and make sure that the answers to this cover all of us. Because as employers, we definitely cannot monitor the hundreds of employees that work for us. And we don't want to find the ability for somebody to come in for whatever reason, take on the employee, and shut down the facility for things like that. So those are the things we're really hoping to get answered in the IRRs.

Answer (Mr. De Rivera): I just wanted to issue a rejoinder to Asec. Sy's earlier statement regarding implementation of the law. I'm wearing my hat as a member of the board of trustees of the Asian Institute of Journalism and Communication. Whereby we are very much in the forefront of advocacy against the culture of impunity, killing of journalists and this sort of thing, I think it's really very important that whatever law we craft, will be crafted, becomes a really good law. On the other hand, it needs to have the implementation done properly including the participation of all of you as Asec. Sy mentioned, so that the culture of impunity can be somehow diminished. People will not take the law into their own hands anymore because they feel that their issues will not be addressed properly. So I think that's a major issue that is also related somehow to what we've been discussing here.

Moderator (Mr. Yu): Thank you Commissioner Tim. Any further questions from the audience? Okay, we do have one question again on… yes. Atty. Salalima?

Answer (Atty. Salalima): This is very critical. The most serious and hotly debated issue in the cybercrime law is the provision on libel, and the section immediately after that provision which speaks of double jeopardy. Meaning that a prosecution under the cybercrime prevention law is without prejudice to a prosecution under the Revised Penal Code. I have heard some legislators say and this does not include my dear friend Freddie, that the reason why electronic or cyberlibel is made part of this law is because allegedly it is not covered by Article 355 of the Revised Penal Code. My fear is it is in fact covered. Therefore, in fact cyber- or electronic libel is already covered by the Revised Penal Code and you are repeating that provision in the cybercrime prevention law, you may be hit by two violations for one and the same offense. Let me explain because it might help our legislators in addressing this cyberlibel. Look at the enumerations in Republic Act… ah in the Revised Penal Code. It speaks of libel through writings, through print, through radio, through cinematographic exhibition. This and it is followed by the word "and similar means" which according to Mr. Sy means the principle of *ejusdem generis* means that several others, similar others would be others of the same nature as those enumerated. Now when you talk of writing, or print, the law does not qualify. That is why electronic writing or electronic print is already part of the Revised Penal Code.

Also, you look at the word radio, in an old case decided by the Supreme Court involving, I think PT&T or PLDT, the Supreme Court said that radio is transmission via airwave or wireless communication. Look at your cellphone, look at your internet, some of them are wireless. Therefore, the word radio already contemplates even our cellphone, which is part of the so called cyber ah… computer apparata as defined in the law. Now look again at the word cinematographic exhibition. The images that you see in your cellphone… these are not the printed words, or the images that we see in the Internet – they are in fact a specie of mass broadcast. In our constitutional law, we have two (2) concepts of mass media: the print media which is the newspaper; and you have the broadcast media which is the radio, which is the television, the cable tape…TV. When you say cinematographic exhibition, this is mass media, this is broadcast mass media. And therefore, when you say "and other similar means," Internet is already contemplated by that because Internet and cinematographic exhibition are both mass media. They are in fact media broadcast. So I am worried about the double jeopardy provision.

Moderator (Mr. Yu): Thank you Atty. Salalima. Okay. Yes. We tend to concentrate on the libel clause. There are others also the data. But I think one thing that came out here earlier today, earlier this morning was that I think everybody feels that Asec. Sy is really a nice guy, you know. Now the point is, including for the Commissioner on Human Rights, when we write the IRRs is we write them to be as protective as possible. We're not saying that this is going to cure the law completely but we have to take safeguards. Let us assume that Asec. Sy is no longer at DOJ, in other words. Perhaps. Do we have a last question? From the audience? Okay, Miss.

Question (Nica Dumlao): Hello. *Ako po si* Nica Dumlao from Foundation of Media Alternatives. *Nagkita na kami ni* Asec. Sy before *sa* ICT for PhD and he is really a nice guy. Now the problem is, the problem is, *paano pag hindi na siya*? *Yun yata yung sasabihin ni* Mr. Yu. *Na paano pag hindi na siya yung nasa* DOJ *and hindi na siya si* cybercrime@doj.gov.ph? So *parang iniisip namin, ano na, ano na yung mangyayayari*? And the thing is, *ang tinatanong, sinasabi kasi namin sa*, I mean, *ang appeal namin sa* DOJ is *huwag munang mag-ano, huwag muna tayo mag*-IRR. *Mag-usap muna tayo kung tama ba talaga ang batas, diba*? *Mag-usap muna tayo dun kasi… ano, tingin namin, kakasabi lang nga ni* sir*… na hindi talaga, hindi talaga masasagot nung ano eh, nung* IRR *yung mga* imperfections *ng batas*. And in the end, *baka mamaya… ano, parang nagawa na natin 'tong mga prosesong 'to…. Sampal din 'to sa mga tao*. *So yun lang po*. *Ang tanong ko lang kay* Sir Sy, *na kung ano ba talaga yung gagawin ninyo*. *Kasi* questionable *'tong batas na 'to eh*. And I think you know that.

Answer (Asec. Sy): Thank you. The good news is I still have 30 years in service before I retire so hopefully we'll build up the institution, enough time. The better news is when I'm personally gone, there will be a nicer guy who will take our places here in front and hopefully that will be the history of the Philippines. But going to your point, yes, that is a very ideal approach. We will try to do what we can. But of course, we also are required to come up with the IRR in 90 days. So it's a catch-22 phrase. Hopefully, we'll have an ideal law, or a better law, amended law. We all want that, not only in this law as mentioned but in all our laws which we have not measured. We measure how well a person dresses, how a senator looks good, but we never measure our quality of laws. We don't have indicators for… it's a good law, it's a bad law, if it meets the criteria of regulation. So, we'll try to manage the process. It's a process of change that compels and requires us to come up with a very good IRR to do our best to harmonize – not to cure, or to fix, or to remedy – we are the principal law agency. We know the law, so we would not try to do anything over, beyond the law. At the same time, being much attuned to the Supreme Court petitions, to the pending legislations, how can we harmonize it? Make no mistake, the priority is going after transnational organized crime. The Department of Justice is up there with the Commission on Human rights in protecting civil liberties. So those are the bedrock of principles that we will adhere to. Thank you.

Answer (Mr. Roxas-Chua): I just want to make comment that this is definitely a landmark bill because of the topic that it covers and I actually have a… I feel good and bad about it. Good because we've been pushing this for so long and we really need it. In the last Congress, I really pushed for it very hard. But it didn't get passed that time. But now that it's there, you know it really brings us, brings the whole country into the digital age. But of course, you know, like any other laws, it's not always perfect and the process is not perfect and what ends up is not perfect. So that's what I think we still have to thank Asec. Sy for organizing this forum, for letting people air out their grievances, and for pointing out the criticisms in an intellectual forum so that steps can be taken to improve it. Not just, you know, posting criticisms without being able to get responses. So we have to thank Asec. Sy for that. He seems very dedicated to making this law work. I think… to end this on a positive note, I think you know we're very happy with the feedback from the affected constituents and we'll just continue to work together with further dialogue to help it work. Maybe there's not going to be an easy solution. The IRR won't cure everything, maybe amendments are necessary down the road but the first step is the dialogue and I think this is a better good first step.

Moderator (Mr. Yu): Okay, thank you Commissioner Ray Roxas-Chua.

We'll have a short summary. Thank you to the panelists.

Emcee: Thank you to our panelists and our moderator. After a brief summary of this by Mr. Dondi Mapa, we will have our photo ops. So please stay for that.

Mr. Mapa: Okay. Good afternoon everyone. Again, I'd like to bring this to a close by summarizing some of the salient issues that we've discussed. I know that there are still a lot of questions and we'd like to have this as a continuing dialogue. There are several venues for you to be represented in this dialogue. Again, I encourage you to join organizations such as the IT Association of the Philippines or ITAP; BPAP is also represented here, as well as PSIA, and the Internet Society Philippine Chapter. However, as promised by Asec. Sy earlier, all of you, all of you are invited to participate in this dialogue, in your individual capacities. Just send an email to cybercrime@doj.gov.ph. Again, the email address is cybercrime@doj.gov.ph, for us to continue this dialogue and to continue this engagement with you, especially as the DOJ begins to craft the IRR or the implementing rules and regulations. I think one of the realizations we have is that this IRR are going to be very important in defining some of the vague terms that Atty. Rudy was referring to, in curtailing some of those powers given to the DOJ under this new law. And I think those IRR's will be our legacy to our next generation of Filipinos. This law will continue to be there and will outlive us and I think if you look at this as our contribution to the next generation of Filipinos, to those Filipinos who will be growing up in the knowledge age, in the information century. This is really our way of making sure that Filipinos are protected in cyberspace. And Filipinos are not taken advantage of by cybercriminals from outside our borders. This is our way of making sure that our Philippine Digital Strategy can really bring the benefits that it has promised to our population. So in closing, I'd like again, to once again say thank you to the Department of Justice and to the ICT Office of DOST for organizing this forum. But most of all, thank you to all of you for participating. Good afternoon and God bless.

Emcee: So, yes, thank you again. On behalf of the Office of Cybercrime from the Department of Justice, and the ICTO-Department of Science and Technology, thank you again and we hope you have a wonderful afternoon ahead of you. We're now going into the photo ops. So please join us in front, may we call on everyone. Thank you.

###