

FINISHED FILE

ASIA PACIFIC REGION INTERNET GOVERNANCE FORUM
TAIPEI 2016
A NEW INTERNET ERA

28 JULY 2016
ROOM 402 (C-D)
16:00
MERGER 3

FOSTERING FREEDOM ONLINE:
THE ROLE OF INTERNET INTERMEDIARIES -
A LOOK AT LEGAL AND PRACTICAL CHALLENGES IN ASIA

Services provided by:
Caption First, Inc.
P.O. box 3066
Monument, CO 80132
800-825-5234
www.captionfirst.com

This text is being provided in realtime format. Communication Access Realtime Translation (CART) or captioning is provided in order to facilitate communication accessibility and may not be a totally verbatim record of the proceedings.

>> KYUNG SIN PARK: Hello. Test, test. Can you hear?

Good afternoon. We are here to talk about the role of intermediary, and in talking about -- intermediaries, and in talking about that, we will use as a text for students, sustainability always nice to have a textbook -- a text -- a research product that just came out of a collaboration between Canadian Centre for Law and Democracy, and the Indian Internet Centre, the Centre for Internet & Society and also Center for Studies of Freedom of Expression and Access to Information at the University of Palermo, that's an Argentinean think tank, and also Public Policy Clinic and also Canada base of Global Affairs at the University of Toronto. The final product is titled Stand up for Digital Rights, and as moderator, I'll first go through what the final recommendations are, and you can listen to them carefully and see if they are appropriate recommendations, especially industry reps, the recommendations go to you, so, you know, it will be interesting what your reactions are.

And also, the experts on the panel were requested to read them and respond to them as well. Okay. The recommendations are divided into six categories. The first is expanding access, expanding people's access to the Internet. The second is net neutrality. Third is content moderation. Fourth is privacy fifth is transparency, and sixth area is responding to state censorship, so the recommendation under the

first area, which is -- okay. I'm not making this up. Okay. Just imagine you are sitting by the ocean.

(Laughter)

Sounds like waves, yeah.

So for expanding access, can you click on the expanding access? Okay. Yeah. Let's just go on. Okay. Can you click on expanding access?

Yes. So the recommendation for expanding access, the first one is on infrastructure. Can you go down? It's small letters. Internet access procedures should invest a reasonable proportion of their profits in expanding the infrastructure for providing access to the Internet, particularly so as to reach underserved communities, including potentially through entering into public-private partnerships to advance this goal.

And also, cost measures. Internet access providers should consider funding or otherwise supporting programs or schemes designed to support access for poorer households, and Internet access providers should work to mitigate or eliminate pricing differentials between rural and urban customers.

I'll just read on. On accessibility, private sector online intermediary should program the development of content of relevance to less connected communities and/or in smaller languages, and awareness raising in those communities and language group about the potential for Internet. And intermediaries should promote accessibility for the disabled by adopting the worldwide web consortiums web content accessibility guidelines. Other issues, Internet access providers should make reasonable efforts to monitor attempts by governments to adopt legislative rules which unduly undermine the expansion of access to the Internet and should engage in or support awareness raising and advocacy efforts to combat such moves. These are very tough duties we are asking the Internet providers. We're asking them to lobby against anti-access government measures. Finally, Internet access providers should never cut off access or deny service to a user unless required to do so by a clear and binding legal order.

Around the world we find many times -- we find many times the Internet service providers cut off the access, even when there is no legal binding order from court, even at the suggestion of some high officials, access is cut off. We are recommending against that.

The second set of recommendation on net neutrality, I'm not going to go through all of it because some of them is basic, but -- can you go down a little bit more. The first set is Internet access providers should respect net neutrality. Let's go to the second set. Net neutrality and expanding access. This one concerns zero rating, so see what we have got here. Programs to expand access to the Internet, which offer a tradeoff in terms of services or connectivity should be designed in an open and nonexclusive transparent manner which respect net neutrality and the right of users to choose what material they wish to access. For such programs, the goal of giving the access provider a competitive advantage should not undermine the broader goal

of connectivity.

Okay. The second recommendation probably is much sharper. Programs to expand access that employ zero rating i.e., provide free access to certain select applications or services should be avoided unless it can be demonstrated clearly that these are significantly more effective than similar programs which do not offend net neutrality. Access providers which offer such programs should make available information about their effectiveness for purposes of independent verification.

So the idea is that zero rating can be permitted, zero rating is permitted, but the companies providing zero rating have a formative duty, has the burden of proving that the zero rating expands access -- is it my location?

(Microphone is buzzing)

Is it my height?

(Laughter)

Okay. All right. The next set of recommendation is on content moderation. I just will talk about the ones that are salient. On clarity and communication, look at the third one, look at the third recommendation on content moderation. Policies to address problematic content such as deletion or moderation, which go beyond the formal legal requirements, what we mean by that is there are unlawful material that are moderated, but there are times that the service providers -- there are times that platforms take out lawful content for quality purposes or just to -- or for marketing purposes or not to offend other users, okay, so when the platforms do that, that should be done according to -- it should be based on clear and predetermined policies which can be justified, referenced to a standard which is based on objective criteria, you know, such as -- such as, you know, just letting everybody know that this is a family-friendly service, right? If you just promote that this is a family-friendly service, the platform's power to take out the content should be expanded -- that's what we are saying -- which are set out in the possible and which is not based on ideological or political goals. Where possible, intermediaries should consult with their users when determining such policies. And the process for receiving and adjudicating complaints, we have a recommendation on that.

So on the second one, they should have in place process to track abusers of their content moderation systems to suppress the voices of women and other minorities, they send a lot of complaints on their postings. And because of the amount of complaints, sometimes women's postings or accounts are shut down, that's what we mean by abuse. So should apply more careful scrutiny to claims from users who repeatedly file frivolous or abusive claims.

The second recommendation, the notification -- this one -- no, there. Yeah, the notification should include a reference to the legal or -- notification is when you take out -- when you take down a content, you send notification to the user. That notification should include a legal or policy procedure being applied and the opportunities available to the user to provide input before a decision is taken and

common defenses to the application of the procedure.

And the last one -- I mean, the next one.

Where possible -- here. Where possible, subject to reasonable resource and technical constraints, users should be given a right to appeal against any decision to take action against a content at issue.

I know that not all platforms give right of appeal to individual content takedown. We are recommending that for each takedown there should be right of appeal for the person who posted it. And on restricting content.

Where -- this one. Where action is taken against content, the intermediary should, subject to reasonable technical constraints, retain the means to reverse that action for as long as the appeal against the action remains pending.

The further set of recommendations is on privacy, so maybe you can click on privacy.

On privacy, communicating with the users -- there. Intermediaries should public clear and transparent information about their policies and practices regarding the collecting, processing, and sharing of user information, so note that the recommendation is not just about private information but all user information, so yes, for public information, the platforms have a lot of freedom to use it without consent, but still, if you are using it, should let the users know how it's being used, even if it doesn't require consent.

The second recommendation, intermediaries should make sure that any representations they make to users regarding privacy or anonymity are clear and -- clear and reasonable and they should then respect those commitments.

Let's go to intermediaries, they should take into account the human rights impact of real-name registration policies and should work to mitigate any negative impacts, including by allowing use of pseudonyms or by allowing parts of the service to be used anonymously. We spent a lot of time why a mandatory real name law is bad, but in jurisdictions where there is no such mandatory law, some companies choose to run their services on a real-name basis, but if you do that, there is a human right impact. And last one is on right to be forgotten.

The third recommendation, search engines should respect due process when applying the right to be forgotten, if they have to, including by informing those whose -- informing those whose content is subject to a removal request, as far as this is legally permitted and by giving them an opportunity to argue that the material should not be blocked, including because the public interest lies in continuing to display the content, and consideration should be given to putting in place some sort of appeals or reconsideration mechanism.

As far as I know, there's no platform right now who gives right of appeal owner right to be forgotten requests. Correct me if I'm wrong. I think this is something that all platforms should think about.

All right. The fifth set is on transparency. I'm not going to speak much about it because we had, like, a couple sessions on transparency already. We are basically recommending the -- all platforms to -- all platforms and network operators to public

transparency reports.

And the last set, maybe you can come out -- yes. On state censorship. Let me just look at the third set, pushing back. Right.

Intermediaries should notify the -- if you look at the second one, intermediaries should notify users who are the subject of a request from a state actor as soon as they are legally allowed to. Many -- in many jurisdictions, when platforms receive takedown orders from the governments, formally, informally, they take it down without notifying the person who posted that content, and I think that is a (Inaudible) to the role of the Internet. So I'll stop here. So I just covered salient points of the recommendation, or I'll say controversial -- possibly controversial points.

If you want to -- during the session, if you want to read more carefully, there is a URL at the top. If you just take the top URL, then, you know, you can then go down to look at the detailed parts of the recommendation.

Having introduced the recommendations, I want to -- it's time for the experts to respond to the recommendations and also give us insight about, you know, what other recommendations they can make. We'll go in the order of seating here, so Professor, can you go first? Yes.

>> PANELIST: Okay. This is an issue that I had worked on sometime back, and I really feel like Brooklyn said he was the youngest guy in the room, not the oldest guy in the room, and now I'm the oldest guy in the room along with Marcos and Paul.

This is an important subject because actually, it impinges a lot on eCommerce, it cuts across eCommerce, and it has to do with the fact that eCommerce platforms are intermediaries. Actually, the issue is limited immunity for intermediaries and how do you handle limited conditions for which they should be accorded immunity?

This report goes beyond that. This report actually suggests some of the duties or tasks that intermediaries can embark upon, but let me talk only about the immunity part of it.

The first country in the world to have immunity for what we call network service provider was Singapore. It was the first law in the world to immunize both civil and criminal laws, but it's limited only to network service provider, it doesn't say intermediary, it says network service provider.

The U.S. came in a few days later, literally a few days later, and they immunized civil liability totally, if you're an intermediary, you're immune, entitled civilly, including defamation law, so there are cases where content was left up there and then when the person was defamed, put a note to the company question, in the case of AOL, AOL literally sat on their hands and didn't do nothing. Nothing was taken against AOL.

So I see -- I see something like this as trying to balance the competing interests of -- of the intermediaries but also potential victims, those that can be harmed from content.

So let's talk about areas that this comes in. TripAdvisor, I'm sure many used, I assume, on this trip.

Amazon reviews, these all have intermediary roles, and the question is what if a review is erroneous, should TripAdvisor or Amazon be held liable. The trend is to say you're given -- you're given some immunity if you remove the content within a specified number of days.

In the case, however, it means there's total immunity for Amazon and TripAdvisor in the U.S. In Singapore, TripAdvisor and Amazon would not be immune, but the carriers would be immune. This is part of the service for TripAdvisor and Amazon.

So where do we sit on this issue? It is really moving to balance competing interests. I mentioned that. I think it was immunizing civil liability but not criminal liability, generally civil liability, which means actual actually defamation law (Inaudible) so some immunity there, but also some notice takedown, meaning that you are -- (Buzzing in the microphone (Inaudible) and Yahoo tells me it takes five days to move content globally because of how this (Inaudible) globally, souptofivedays. I see this report as trying to balance those competing interests. What is new in this report? Like I said, the recommendations, they go beyond immunizing intermediaries for liability but going beyond to talk about some positive duties (Inaudible), and that I think is what we're to discuss. Thank you.

>> PANELIST: Thank you. Next, Sarvjeet. Again, five minutes.

>> SARVJEET SINGH: Hi. My name is Sarvjeet Singh --

(Audio technical difficulties)

-- almost 280 million use -- Facebook has over 150 million users in India and (Inaudible) has around 30 million. By any measure, these are huge numbers, and (Inaudible) how people access information and communicate with each other. And while it is important that we are -- while it is important that we hold the states accountable if they interfere with our digital rights, (Audio technical difficulties)

Most of these countries aren't allowed to operate in China, India, if they can get a lot of people connected --

(Audio technical difficulties)

-- any kind of zero rating violates the freedom of expression, and that's guaranteed under the Indian constitution and international civil and political rights. In India, only about 12% of the population speaks English, only 65% of the content is available in English, and a large number of languages or dialects remain unrepresented, and the other thing is that they need to partner with local institutions to bridge the gender and rural and urban. Like in India, only 29% of users are women, and this is reduced significantly to only 12% in rural areas.

And the other major area where the Internet intermediaries should take a leading role is to make sure (Inaudible) recently we have done some work with access now and have documented around 28 instances of shutdown since 2015 out of these, 14 instances have been recorded just within this year, and the longest been almost 19 days, so for almost three weeks, people in the state did not have access to Internet or mobile phones, and that -- apart from just restricting I would say the freedom of expression, the other thick that it does, it also has a negative economic effect, and that's where possibly the Civil Society

organizations, the Civil Society organizations, the advocacy groups, and the countries can come together and demand answers from the government and maybe put a legal challenge against this.

To quickly go through the content -- I'll just start --
(Phone ringing)

>> KYUNG SIN PARK: (Inaudible)

>> KELLY KHA YEUN KIM: Okay. I'm Kelly Kim from Korea. In regarding the recommendations for responsible tech, especially recommendations for content moderation and recommendations for privacy have particular importance in Korean case, so may I give you a brief background, regarding content moderation. Our law allows online content moderation in two types. First is on auto censorship, I (Inaudible) Korea Communications Standard Commission, KCSC. This KCSC shows more than 100,000 correction requests that are actually content removal requests under the Sound Communication Ethics or this KCSC can make requests which they claim to be not binding to Internet intermediaries to take down these contents that are in violation of, like, sound communication, ethics.

Although they claim -- they claim -- although the requests is not binding, it has almost 100% compliance by the intermediaries.

And second, content removal in response to private parties' request, according to the Information and Communications Network Act, anyone can make a request to intermediaries to take down contents that are infringing on his or her rights, something like that from privacy content, and similarly, under the copyright act, anyone can request intermediaries to take down allegedly copyright infringement contents.

Although the law can be read as providing Safe Harbor to the intermediaries, something like (Inaudible) Copyright Act of the U.S., Korean intermediaries have chosen to interpret the law as amended requirement, so essentially the takedown under the information and communications network act, many public figures, professionals, and celebrities use this notice of takedown or request -- a private party request takedown system to take down any unfavorable information about them online, so I must say this is much powerful than the right to be forgotten, which is just a right to request an intermediary to delete content about somebody, so as a resort, the intermediaries are forced to take down thousands daily, even though they feel it's lawful in Korea.

Second, regarding privacy and mass surveillance, Korean laws, surveillance laws are in general not dissimilar from other countries except the state notice to those under surveillance are delayed until the end of the investigation, after the indictment decisions are made; however, like overbroad surveillance requests are often filed, and regarding online anonymity, user identity requests or subscriber identification data request issues is very concerning in Korea. Our Telecommunications Business Act allows intermediaries to recall subscriber information, like identification data to the investigative authorities without a warrant or any judicial order and without any notification to the users.

And the intermediaries always nearly comply, even though the

requests -- I mean, the request is not mandatory.

Well, a silver lining here is the largest (Inaudible) have to comply with the request since 2012 following a court decision; however, the problem is that (Inaudible) to comply, and the numbers -- the number is actually growing, and about 13 million people's ID information was given in year 2014 alone, and Korea is a country with, like, 50 million people.

So regarding surveillance, intermediaries have a very narrow ability to exercise any right favoring discretion; however, it is -- as I just mentioned, this leading intermediaries like Naver, Kakao and Google have kind of fought back against those known mandatory subscriber ID data requests and they focused more on published -- they're focused on publishing transparency reports and favoring technologies, so as you can see, our Internet intermediaries play a pivotal role in delivering human rights in Korea, and many of the restrictions on free speech and privacy come in the form of law, and the -- many of the principles of the media library was published in March last year has been very helpful for us, our Civil Society, to fight against Draconian Intermediary Liability in Korea, and these recommendations -- I must say it's much more ambitious and comprehensive than the many principles, but I think it can be a very good guideline for both the Civil Society and the Internet communities. Thanks.

>> KYUNG SIN PARK: Thank you.

>> PANELIST: Hi. A couple of different points.

I'll pick on the privacy points more than any of the others because the others have covered consent and -- I'm sorry, content and takedown and other things really well.

I wanted to make one sort of preliminary point that even though this report actually focuses on the private sector, I would actually urge that it also apply in principle to Civil Society and to NGOs because I find that post-Snowden there was a lot of pressure on the data on surveillance, but the one section that remains visible and handles very sensitive things by people, are human rights organizations, aid development organizations working in different countries who often deal with things about health, identity schemes, welfare, and benefits and the ones with the best intentions are not aware of privacy security trends and policies, and the assumption is always that they're the good guys and, therefore, we shouldn't pick on them, but this is to help them do their work better because if they're putting their data in an unsecured way or putting something in the Cloud or if they're not anonymizing information to the extent it can be anonymized, which we all know is like believing in Santa Claus, to some extent they're putting the very users they're seeking to help at risk, so I think it's not for lack of knowledge. You know, the social scientists and health workers and development people. They're not thinking in terms of encryption and security. Whether you use Google Docs, whether you use something else, what products and tools and services have been vetted for your particular threat model, especially since there isn't a one size fits all thread model for the world. I would urge that in a lot of the work that I've done, people tend to think I'm not dealing

with data, and you think look, have you ever touched a computer and a phone in your life?

You're dealing with data.

So I think to keep reinforcing that you don't have to be in the IT sector, you don't need to be Google or Facebook to take on these kinds of responsibilities, if you're handling people's information, you should be bound by rules like this. To sort of extend the scope of this report, to help people and I think investigate them and say they're not doing their job, but give them the resources, training, and the tools to actually help them implement a lot of these safeguards for very vulnerable populations at risk.

So the other couple of points I wanted to make is a lot of the recommendations in the report on the privacy section, I agree with a lot of them, but I think many of them, the critique I would have -- I have a couple of critiques. One is they sort of push a lot of the responsibility back on to the user. I would urge that a lot of the responsibility for implementing privacy and security rests with the platform in terms of the architecture and the design, and it's something that came up in the morning as well when we had a panel on Internet architecture and human rights. You know, the whole idea of who is infrastructure and the database and the human rights implications of that, and I think in the same way of proxy services or masking services, if they want to remain with some anonymity or flexibility online, you have to pay for those services. I think in the same way this report also seems to ask that intermediaries give options for people who don't want their data to be used where companies use data as their business model, they should give an option for people to opt out and say, well, charge me instead.

And I think that sets us down a dangerous path. I don't like the idea of treating privacy as a luxury good. I don't like where some people can access privacy because they're willing to pay for it and others are not. I would say the default position would be you don't collect the data unless you absolutely need to, that it should be necessary and proportionate, and I the report does a good job of saying what those finally grained criteria are, I just have a bone to pick with the idea of saying give people the option to pay for it because I think you will end up with a really distorted world if that happens.

There are others that have talked it even in the west, like Julie that have talked about privacy as a luxury, but that's salient in the rest of the world, like where we are right now.

The other thing I wanted to point out, when we're talking about privacy policies and terms and conditions and communicating to users, being clear, being unambiguous, which is hard because they're complex transactions because you're sharing information with a whole lot of people. On one hand you want to give information and be transparent, on the other hand you want to be able to let them read through your privacy policy. I say this as a lawyer who has drafted a lot of these docs. Do you make it simple and readable? It's a balancing act. They say that privacy law or even privacy policies are tasked with work

that's beyond their capabilities. We're expecting a privacy policy to set a standard, to set a -- sort of raise expectations, but you're expecting people to read them, understand them, and we're sort of ignoring the set of cognitive deficiencies and biases that are inherent. For example, you ask for consent and people believe consent is like this magic wand that you wave and everything is okay and you can do what you want because people have consented. The second you begin to unpack it and say is it really informed consent, did they click through something because they were desperate to pay for the concert ticket ten minutes before it started, did they even know what they were signing up for?

In that context he talks about reasons why consent is fundamentally broken, and one is about the fact there's a temporal issue. You ask for consent once; you ask it up front. People consent at that single point in time because at that point they think the tradeoff they're making is a valid one. I'll give you this information for the trade-off, that's fine. Right now I need this desperately. They're not thinking about the actors who might come in contact with the data, none of whom they'll ever know about. They have no visibility of the entire set of ecosystem.

So that's one problem. I think there's also economics that's helpful in people nudging around these. So I'll close that.

>> KYUNG SIN PARK: Thank you. Thank you for the insightful comments directly on the recommendations. If anybody in the audience or on the panel also makes comments directly on the recommendations, you'll hear this compliment again.

Last but not least, we'll hear from one of the intermediary's representative herself, Ankhi Das, from Facebook. By the way, because I was distracted by the noise, I forgot to introduce people on the panel. Ang Peng Hwa from the Nanyang Technological University; Sarvjeet Singh, Senior Fellow and Project Manager at National Law University, Delhi; Kelly Kim from Open Net; Malavika Jayaram, she is newly appointed executive director for Digital Asia Hub, which will be a think tank to respond to various issues coming out of Asia, so please give a round of applause to the panelists. Which we forgot at the top of the session.

(Applause)

Now, Ankhi, go.

>> ANKHI DAS: Thank you. So I'll reflect on a couple of the principles which got covered in this -- your opening statements, and I'll sort of touch upon access and also respond to some of the points that you raised, Sarvjeet, and of my five minutes, I'll use a minute to talk about content moderation. So in terms of expanding access, as a company we are making appropriate investments in terms of improving last-mile access infrastructure, which is a very major problem in India, as well as -- as well as in the South Asia region.

There's a real need in terms of investing in last-mile infrastructure, and whether you like it or not, 95% or even more of those investments are coming from the private sector. That is something which we just have to -- it's like the morning sun, we just have to

recognize that fact.

In terms of the investment we as a company are making, in terms of the last mile infrastructure in the industry -- this is something that has gained a lot of currency which is public Wi-Fi, and our express Wi-Fi program is essentially creating village-level entrepreneurs to be able to provide last-mile public Wi-Fi access services, and the main problem is we are trying to solve there is that what is the sustainable business model, what does it look like to provide this last-mile access infrastructure?

We're also working on something that principally has been provided in rural areas. We're also working on something which is described as a Terragraph project, and that again looks at providing last-mile infrastructure in very congested towns where there is a gap in terms of typical mobile Internet being -- operators being able to provide that type of access infrastructure. Just last week we had -- we had an event where our first solar part -- plane, unmanned aerial vehicle completed its test flight, and the goal is to sort of take that to scale after some other test flights which are concluded and use that -- use that device to service areas which cannot be connected by traditional operators and by traditional mechanisms, so those are the kind of things which we are doing on the access infrastructure side.

At the same time, there is this big problem of affordability and relevance, and the report here recognizes that there are different types and different kinds of zero rating. To the extent that zero -- there are innovative business models or innovative business arrangements which are open, nonexclusive, and is equally accessible to all developers to access, those kinds of zero rating should be permitted, and they are legitimate, free development, the free basics app. There was, of course, this long history. As you know, we have lots of stories from India to share from that, but Freebase access and applications is live in 44 countries and it's working and we have presented data. You talk about the burden of proof being on platforms to establish that. It is actually bringing more people online, and we've placed data in the public domain where we have established that in excess of 25 million people, connected people online, and that has been shared and put in the public domain, so that's what we are doing on the investment side in terms of expanding access and connecting the next billion.

On the content moderation -- on the content moderation side, there's some very well established principles which have been recognized in the report from a Facebook perspective. We take this very seriously. As you know, we are a GNI member company, and we are required to conduct independent assessment of our compliance with GNI principles and on free expression and privacy both, and we participate in that. We also regularly engage with Civil Societies' communities as well as are forever expanding the network of engagement which we have with Civil Society actors, experts, think tanks, we public a transparency report twice a year and are very open to feedback. Every cycle there is improvements which is added in terms of the transparency report.

We also feel that our products themselves are important tools for counter speech and for advocating for human rights, and there are various programs which we are designing with community groups, with millennials, with Civil Society to make sure there's broader awareness and recognition as to how you can use counter speech to shine spotlight on bad legislation or bad trends, also the types of mobile Internet bans which was talked about.

>> Thank you. So what do you think, do you think Facebook has met the burden of showing free basics expands access, Internet access?

Yeah. Okay. We have another set of recommendations in the form of template notice that intermediaries or content platforms can use in notifying the users when they take down the content, or the notice template that the users are required to use or the complainants are required to use in requesting takedown.

We'll hear from someone sitting far from here, Jeremy Malcolm, at Electronic Frontiers Foundation, so -- okay.

>> JEREMY MALCOLM: Hello, can you hear me?

>> PANELIST: Can you hear us?

>> JEREMY MALCOLM: Yes, I can hear you, and hopefully you can hear me too.

So I'm not sure if I am able to advance the slides myself, so perhaps someone can do that to me if there's not a way for me to do it.

>> PANELIST: We can manage it, so let us know when you want to go to the next page.

>> JEREMY MALCOLM: We've heard a little bit about the principles on intermediary liability already, and it's not a project that's just been finished and we've moved on. In fact, we're continuing to work to improve the resources available through the Manila Principles website, and one of those is indeed this template notice to users when their content is restricted by an intermediary, often at the request of a third party.

Now, I'm not seeing the slides on the screen. Can be done about that?

>> PANELIST: Okay. You are on the first page. You are on the cover page.

>> JEREMY MALCOLM: I'm not saying anything.

>> You made it. You need to see it yourself now?

>> JEREMY MALCOLM: Okay. Never mind. As long as you can see it, that's the main thing. So that's fine. So let's just move on to the next slide, which is the outline, and so I'll just be giving a little bit of background about why we did this, and then I'll be leading you through the notice itself.

>> PANELIST: Okay. Next slide, please.

>> JEREMY MALCOLM: We can skip ahead two slides until we get to the colorful table, which has the heading How Are Users Notified of Content Restriction, so I'm assuming that --

>> PANELIST: Yes, there is a colorful table. Go ahead.

>> JEREMY MALCOLM: So one thing that we found in looking at the some of the jurisdictions around the world is that there's no consistency

about when users have to be notified about their content being taken down for various reasons.

It's very seldom required by the law that users receive any notice at all when their content is taken down, and so here's a little table which illustrates that for five of the jurisdictions around the world.

The most common case where users do have to be notified is where their content is taken down due to a copyright claim, but for other sorts of claims, hate speech and privacy, they are not required to be notified when their content's taken down, and so therefore, they don't -- there's no incentive for the intermediary to warn them about that fact, and if they have any disagreement with the content being removed, they're not -- they're not given any opportunity to object.

So we -- the worst-case scenario is where there's even a limitation on them even being notified that their content has been blocked, which is possibly the case for the right to be forgotten removals in Europe.

So we thought that this was a bad situation that should be addressed. Can you move to the next slide, please.

One of the other problems that we wanted to address was in the case where -- where users' content is restricted under a legal process such as the DMCA, they may be notified, but not when the same content is removed under the intermediary's terms of service. We wanted to make sure that these very similar situations were treated in the same way; in other words, that users should be notified when their content's removed, no matter whether it is removed due to a legal procedure or due to the internal application of terms of service. The effect on the user is the same, so they should be notified in the same way.

Another problem we wanted to address is that intermediaries were simply forwarding notices that rights holders were writing to users, which may have been completely inaccurate, and there's an example of this in the case of Canada where copyright owners were sending notices via ISPs that were completely inaccurate and claimed that users would be liable to U.S.-level penalties when that wasn't the case because they were Canadians, not Americans.

So what we wanted to do was to try and make it easier for intermediaries to send out a notice to their users that would be accurate and that they could use for both when they're following a legal mandate or when they're applying their own terms of service, and the Manila Principles do provide for such a thing, if we can move on to the next slide. The Manila Principles do say that intermediaries who host content may be required by law to forward a lawful and compliant request to the user. When forwarding the request, the intermediary must provide a clear and accessible explanation to the user's rights, including any counter notice or appeal mechanism, so the Manila Principles suggest the intermediaries do that, but they don't provide a template, so what we decided to do was provide a template that the intermediary could use to generate a suitable notice for the user when the content has been restricted.

So let's skip ahead two slides. Yep. And the next one after that. Where we will see just the first part of the -- oh, no, I think there should be one -- there's an orange slide.

>> PANELIST: Yep. We are seeing it.

>> JEREMY MALCOLM: I think you've gone too far. Just go -- yeah, there we go. So this is just part of the form. I'll give you the web address of the complete form, but this is just the first few fields of the form. You can see here you fill in who made the content restriction request, in other words, if someone's asked for a user's content to be taken down, who were they, when did they make the request, where was the content found originally, that sort of thing, so there's about -- it's a single-page form. It's not that long, and the exact fields that you see will change based on your answers, so you may be asked is this a copyright complaint, and then you'll receive further questions that are relevant to that, and so the exact format of the notice will vary, depending on your answers in this form.

So moving ahead again to the next slide. This form is meant to apply to different areas of law, so if there's a complaint that the user's content infringes copyright or is defamatory or infringes someone's privacy, it's meant to be applicable for all of those reasons, and it's also meant to apply to different legal regimes, such as a notice and notice regime, a notice and takedown regime, and as I said, where there's an order from a court to take down content or when it's simply a decision of the intermediary to take it down under their terms of service. And finally, it's meant to apply in different jurisdictions, different legal systems such as common law or civil law jurisdictions, so for this reason, it is pretty general, and we fully expect that it might be necessary to fine-tune the -- the results of this -- the outputs of this form before it's sent to the user, but nonetheless, it does provide a convenient, quick and easy way to rough up a draft notice to the user.

Next slide, please. So just to clarify some things that we didn't intend that this would be used for, we didn't want to try and tell larger intermediaries like Google or Facebook that they should be using our notice generated because clearly they don't need to. They've already got their own lawyers, they already know what they're doing, so this is really meant for the smaller intermediaries who maybe don't know what kind of notification they should be sending to their users.

It isn't meant to be providing legal advice. It's not meant to supersede any legal requirements that specify the contents of a notice to users, which may exist in some jurisdictions, although, unfortunately, they don't really exist in most, but if a country does specify the format of a notice to the user, then that would prevail over our --

>> KYUNG SIN PARK: Jeremy, I know you are a lawyer, but these are like a set of disclaimers. Can you skip them and finish in 30 seconds?

>> JEREMY MALCOLM: Sure. Well, let's just skip ahead to four or five slides, which -- okay. This will do. Show how to use it. The address that you can see there is Manilaprinciples.org/template. You can also find it under the menu that says "resources." If you click on resources and then notice of content restriction generator under that menu item, you'll be able to get there. We suggest that you don't

assume that it's 100% correct. It may still have some bugs, so if you find any bugs, then please let us know.

And then to the very final slide, yeah, spread the word, let us know if you find it useful, and if you don't, please tell us how to improve it, and you can contact me at my email address. It's on the first slide of this presentation, so thanks for the opportunity.

>> PANELIST: Thank you. Just one question, is Manila Principles still open for signature?

>> JEREMY MALCOLM: Yes, it is, and now that we are launching this -- and we've also launched a new blog section on the website. Because of these new things just having been done, we're going to do another push to encourage more people to sign on, so it would be a good time to sign on. If we get a number of new signatures altogether, we'll make an announcement and maybe blog about it. So it would be a good way to get --

>> PANELIST: They're making their headway into (Inaudible) freedom of expression and it's likely to be cited by the special repertoire on privacy as well, and many other UN originated documents, so to add to the impetus, I also urge individuals and organizations to look at the Manila Principles. Let's give a round of applause to Jeremy, who has spoke from afar.

Okay. We have ample time for question and answers. Anyone in the audience? Yes, Chad first.

>> AUDIENCE MEMBER: My question is to Malavika around the responsibility as well of other institutions or organizations that collect data, right? I mean, I suppose the Manila Principles, as I understand it, is for intermediaries, and I ask this question because I think maybe that's much more related to the -- let's say -- I just came -- in the Philippines we now have the Data Privacy Act, and I went to a consultation, and in fact, in that consultation by the government, because there now is a privacy commission -- there were research organizations who did say look, you know what, they're not concerned about what a responsibility is because of the Data Privacy Act, so maybe that's where it was much more relevant, and one thing that they did say was that they have much higher ethical standards in collecting data, protecting data, and working with data. Just a question around why you feel that this is relevant for intermediaries.

>> MALAVIKA JAYARAM: So my involvement came out because I was talking to Hivos about funding they gave to a lot of organizations, and they found they didn't actually implement these principles, so it's actually similar to Rebecca Simmons approach to ranking individual rights. We sort of impose obligations on people to say, look, in the mining industry with diamonds, with minerals, we rate people -- or even diversity, we rate companies and people based on how they implement those rules around ethical practices, so why aren't we doing the same when it comes to free speech privacy, and so it sort of started off with that point of view and was saying that a lot of these people with the best intention in the world were not implementing them because some of it for where it was for anthropological research, you had students going off doing surveys in Africa publishing something online and the

data never got back to the people that actually had generated, they weren't asked for consent, they didn't get a chance to approve it or delete it, so I think one sort of response was there was no feedback loop where the data was actually effectively used by the communities that generated them, there was this predatory relationship where it was -- again, it gets to the point of who really owns data, and if somebody else is analyzing data, does the user have any rights if they didn't generate it themselves?

And I think big data also sort of raises all these questions because on one hand, if you're doing big data analysis, a lot of people's excuse is, well, it's all anonymized, aggregated, so there's no person to search for personally identifiable information, so, therefore, data privacy laws and data protection laws would not actually protect individuals because they're not able to show it was them individually it was their data but it was their membership of a class that made assumptions about them or treated them in particular categories and stereotypes which did affect their life choices. So if they were treated as a member of a class, they may not have got a loan because they were deemed to be high risk, even though that particular person may have been wonderful with their credit.

I think it was in the context we were looking at it, and it was more the point that a lot of the organizations are not thinking about what tools to use, that they put something in the Cloud or if they use Facebook to organize, they don't realize that in particular impressive governments putting all these people's user names and information could be threatening to them, not just Internet privacy but actual physical security. When it's anonymized and there's a village of 15 people and someone has HIV, it's very easy to find -- when you're dealing with health, other sensitive scenarios, even though technically you may not be held to the same standards as a company and even though ethic lip you may be functioning really -- there is an expertise of when it comes to keeping the data safe and secure, and the onward use of that data earn a the people that it relates to, so I think it was in that context that I meant it, it's sort of saying it's not like we expect them to live up to the same standards of Facebook or Google or they have the same public responsibility, but maybe they can start getting there and maybe we should help them get there in some way because a lot of them get hacked, they have data breaches, so for all of those reasons I think they should also be handling data sensitively.

>> KYUNG SIN PARK: Thank you. Next. Yes. Mic is coming from your behind.

>> AUDIENCE MEMBER: Oh, okay. Ms. Malavika, what we do is transparency, and we release names. Names are very sensitive in some case. We have a line. The line is called publicly -- politically exposed person. Sorry. I'm tired. Okay. The point is some people deserve less privacy than other -- we need to know the line. That's one. For us our line is name only and not kids. Okay. Keep it short.

Privacy can -- we need to know the line. Thanks. I need to know what's the --

>> PANELIST: That's the holy grail. Context may dictate that. In some cases, a name might be meaningless, but in India, a name might show your -- your name can immediately identify various attributes about you even though you never talked about them, right, in the way that you know Michael might be Christian and Mohammad might be Muslim, right, it's that kind of thing, but it can be more finally grained like that. In a lot of communities, it can indicate a tribe or something, so I think names can be really sensitive, but I think what you do and don't disclose also really depends on what your threat model is.

The one pushback I would have is that idea of some people deserve privacy more than others. Everyone deserves privacy. There was a really good point where it was said transparency for those with power and privacy is for those without, and interestingly, I sent that to a techie who completely resisted this idea, which I found funny because I expected a legal -- fantastic because I expected a legal person to come back with this response, not a techie person. He said I completely disagree with that, I think everyone should have privacy. I think if you're a public person, maybe you may be in the public domain and maybe the public may have a right to know it, but I think this idea because you're public or famous or a celebrity that you lose to have the right to have privacy in your personal life. We have privacy that I don't think anyone should intrude into, I think we all have those basic rights. I think it's a sliding scale. What's appropriate will be dictated by circumstances.

>> KYUNG SIN PARK: Okay. Yes.

>> AUDIENCE MEMBER: So I'm curious about the Internet access, the material you're put in there. (Inaudible) I was just curious and the focus on ensuring investment in Internet, and I totally get that in terms of it being a critical policy, but as a specific recommendation on the tech sector, particularly because, for example, as you mentioned, and just by background, I worked on some of these projects. I used to work at Google previously. Some models of people talk about it differently, a nonprofit for investment or donation. Those are definitely business models. They might be customer acquisition or some might be for profit. You can talk about the Google fiber projects, many other project that people are deploying, many of the Wi-Fi projects that Microsoft works with. I'm curious why a specific recommendation in that model, and why I ask that is -- I appreciate the -- I probably agree that I won't endorse the text as is, but I'm just curious in terms of why the focus in saying they must invest in the sector because I think it misses the fact that some of them will do it for business reasons, and that's fine, and I would then jump -- I think this has happened some in the UN language and saying human rights should apply online, but other people will say invest in the sector and then say on zero rating this may be the broad test. What I'm trying to say is two concerns, one in saying that you should invest means you take away from the someone with access solutions develop a business model, and that's fine, I think that's okay, and that takes away from the fact that you may have a more specific discussion, say, for example, on drones or balloons, not all will be consumer facing, some will be

back end, and they say privacy should apply or mass collection of data, you know, maybe we need more norms there, so just curious about that because I think we preempted some of the further norm discussion that could happen in the space, and I think we could always have norm discussion, but I'm just curious because this is one important one and this is a slight flare point in the sector.

>> PANELIST: Well, I think as one of the drafters, maybe I should answer. I think that the recommendations were not -- are to be taken as an interweaving with one another, crisscrossing with one another, so -- but we wanted to have one section where people approach intermediary responsibility from corporate -- from traditional perspective where investment is always emphasized. That's -- that's just about concrete answer I can give. There was another question from Winston.

>> AUDIENCE MEMBER: Thank you. I just wanted to come back very briefly to something that Malavika said. You mentioned the case of -- I don't know whether it's a true case or a hypothetical case, but people who might go to Africa to do anthropological research, I think you said, and you said there was a problem with using the data and there would be no feedback to the people who were actually at the source of the data that was put into the study.

It just occurred to me that if that data is done in a proper environment, there are (Inaudible) a project to go ahead, so I'm worried about the example you quoted, if people were doing that and it had not been run past any academic ethics committee, then there was a problem.

It also occurred to me that maybe the people who own data broadly in ISPs should have their own ethics committee, which could judge the validity of proposals or requests to use the data that they control. Maybe they should be forced to create their own internal ethics committees.

>> KYUNG SIN PARK: Okay.

>> MALAVIKA JAYARAM: I think if corporations were to create those kinds of ethics committees -- and I think many have, Twitter has tried to do a Trust and Security Council, but if they do that, I would hope they don't follow some of the bad things that come out in the academic model. I think it's one of the problems on one hand you wanted to use the data and do meaningful research, and I think this comes up with medical data where until you actually start doing the research, you don't know what you're going to use it for. It's only once you've collected the data you think, oh, actually, I thought I was looking at flu, but I'm also looking at cancer, and then do you go back and ask for more consent?

I've been at Harvard for the last three years, and this is something that keeps coming up where the scientists and researchers and doctors in particular are saying if I was to set out my research questions up front, I would be limiting myself. If you don't let me push the boundaries of what I'm doing, it's pointless and I don't know about the data until I get my hands dirty, so they want the freedom and flexibility to leave it as broadly worded as possible, but from the research subject's point of view, it's not wait a minute, once you collect it, you can repurpose it for 27 reasons I didn't actually think

-- you know, I might really care about the flu because my mother died of it, I don't care if my data's used by -- -- I think people have reasons why they would or wouldn't give their data up, and I think sometimes those competing interests get muddled up. The example I used did actually come up.

I mean, we -- with the engine room, with a whole bunch of others, about 15 of us actually worked on a little -- we did a book sprint in five days and actually published a 160-page thing, which is writing a book by committee, which I didn't think was possible. You know, you can barely write one by yourself. We it this and this was an example that came up, they go after Africa, they do research. It's not necessarily in an academic scenario. That's why I mentioned NGOs and organizations where they're not bound by the ethics that an academic institution would have. It's more people little NGOs, can we do a startup looking at incubators for babies and getting them to the nearest hospital. They're not bound by standards, so I was saying could we cover those people on the fringe of academia and on the fringe of corporates and sort of say it's going to take you a while to get there, but how can we handle you getting there and actually help you rather than saying look, you're doing this all wrong and we're going to penalize you. Can we train you, can we say you need to have techie people, you need legal help with templates or documents or just help you -- like access now has a security helpline where you can ring and say actually, help me, tell me what I should be doing, so they can raise a ticket instead of give you a case and walk through what tools and products might be useful for you. I was saying how do we build capacity and bring them on ramp to do the right thing.

>> KYUNG SIN PARK: Okay. Thank you. Question? Yes, go ahead.

>> AUDIENCE MEMBER: My name is Jen Lee from Taiwan. I study open government issues now, so I want to comment on that issue. I agree with a lot of your opinion, and that is really the issue of anthropology, nowadays how do we keep the code between the privacy of the data from the people we work with in our field and at the same time how to make it open and make it responsible for the community that we started with. And I think this might be the similar issues, like to think maybe it's not a good comparison between me and a corporation like a Facebook or something like that, but is there some way that we can think that how a corporation to try to, you know, keep some kind of privacy of the data but at the same time to think what's the responsibility of transparency and openness and how is the line, the tricky line to draw between these two things and being responsible to the whole community, and as an anthropologist, I will do my best to do that and help contribute to this.

>> KYUNG SIN PARK: Okay. It sounds like we are adding another recommendation to the tech companies to create their own ethics committees for big data research. Actually, many private hospitals are required to have IRBs, review boards for conducting any research, including human bodies, and when you do research on live subjects and obtain personal data, that can be considered human body research. So a lot of social science research comes through IRBs for approval, so --

>> AUDIENCE MEMBER: (Inaudible)
>> KYUNG SIN PARK: Google has IRB?
>> AUDIENCE MEMBER: (Inaudible)

>> KYUNG SIN PARK: Yeah. Good. We are still waiting for our last panelist Lih Shiun Goh, representative from Google, but I guess he cannot make it. Well, there was one -- I want -- if he shows up, I wanted to put Lih and Anghi -- put under the spotlight at the same time, but since Lih has not come, I'll put you on the spotlight and ask you this question. Right now Facebook has a right of appeal process for account shutdowns, so if a user account is shut town, their account -- right -- shut down, their account -- right. But as far as I know there is no right of appeal for individual posting takedown or account suspension, suspension for, like, 24 hours for temporary suspension, I believe there is no right of appeal. Having -- you know, having seen the recommendations, do you think it's appropriate for Facebook to institute right of appeal on temporary suspension in individual posting takedown?

>> ANKHI DAS: Individual posting takedown, that's a tricky one, but, I mean it's good input for us to certainly look at, but in terms of the temporary suspension, when we do notice to the user in terms of the temporary suspension, there are very -- yeah, there's very detailed cause of action which is provided there in terms of reasons which advanced in terms of the checkpointing which is done in terms of temporary suspensions, and also the user is provided guidance in terms of what needs to -- what the person, you know, should avoid doing, you know, if the person is violating the committee standards, is there certain things which the person has done which should not be -- which is in violation of the committee standards. Obviously the guidance as provided is generate ago mechanism also. That we feel suffices in terms of satisfying the requirement for the user to engage with Facebook, and I feel that -- we feel that that is an appropriate mechanism which we have.

In terms of individual postings which come down, they come down because of valid reasons, and we've toiled for a while in terms of whether we should be doing notice to users, in terms of individual postings coming down, et cetera. That's a more long-term complicated discussion.

>> KYUNG SIN PARK: So in short, she said no for temporary account suspension.

The -- just for those of who are curious, the question that I wanted to ask Google rep was whether Google is planning to or is willing to institute --

>> (Inaudible)

>> KYUNG SIN PARK: Of course. (Inaudible) is willing to institute right of appeal for right to be forgotten delistings because there is no right of appeal at all for right of -- for right to be forgotten delistings.

Facebook has a right of appeal for account shutdowns at least and has shown up here, but Google has no right of appeal for ITPF, other listings.

Well, we are out of time, but since I took up the last few minutes, if there is any other questions, comment -- yes.

>> AUDIENCE MEMBER: So I had a question for Sarvjeet and Ankhi from their different perspectives. I think you said only 12% speaks English but 60% is out there in English, and you said more needs to be done around that. What is your perspective on the role of intermediaries in fostering that because a lot of it has to come from the ground, has to come from ground up, about you where do large intermediaries like Google and Facebook play a big part in facilitating the sharing of content? Where do you think they fall, and Ankhi, from your perspective, is it the responsibility of a company like Facebook to promote local language content?

>> KYUNG SIN PARK: So in terms of -- if I just take the example of India, I think a lot of these companies are already doing a lot of work and I think they have initiated where they're like teaching people how to use the Internet and providing more local level content, and Facebook I think is available in multiple (Inaudible) which is in India, the only point what needs to be done, I guess it will take a lot of time and more such efforts needs to be made and probably different companies need to come together because that would make it faster and yeah --

>> ANKHI DAS: So I think all platforms are rapidly providing translation tools. I can talk about Facebook, what we recently did. There is a translation tool which we launched on the Android version of the app, which is the most pervasive platform, which is there on mobile, and that has been helpful in terms of driving conversions in terms of just helping people.

The main constraint, the main challenge which we've seen in India in terms of the net user base of people who are connected to the Internet, majority of them are on feature phones, and the main constraints from an input factor perspective is the lack of local language keyboards. It has been -- it's very important for people to understand that constraint factor. People just assume that the entire country is on smartphone, it is not, and that is, in fact, correct for much of South Asia, so the phone OEMs need to make sure that the input factor by way of a local language keyboard is something they're actively working on, not yet in terms of something of a detachable local language keyboard for a variety of reasons, it didn't take off, it didn't do well, so if there is no sale market in that kind of stuff, companies stop investing in making that. That is the main constraint factor. What we try and do is work with phone OEMs to see if they can preload local language forms. These things take time. What we can do on the platform side, we are doing. All platforms are doing it. We are doing it. It will take a while.

>> KYUNG SIN PARK: Okay. We are out of time, and there is exciting -- since there's a document session waiting to happen right now, and right now, thank you all for coming, and thank you to the panelists.

(Applause)

(Session concluded at 5:34 p.m.)

This text is being provided in realtime format. Communication Access Realtime Translation (CART) or captioning is provided in order to facilitate communication accessibility and may not be a totally verbatim record of the proceedings.
