FINISHED COPY

ITU - AI for Good Global Summit session: Breakthrough Groups on Privacy and Ethics - Enhancing Privacy and Security
JUNE 8, 2017
3:30 AM CT

Services provided by:
Caption First, Inc.
P.O. Box 3066
Monument, CO 80132
1-877-825-5234
+001-719-481-9835
www.captionfirst.com

****

****

Please stand by. 1, 2, 3, 4, 5.

>> We will start in one minute. Hello, everyone. I think we can start the breakthrough session now. We have only one hour and a half until 12:00. We have a lot to cover. We have wonderful panel members with us. Sean McGregor and I'm the moderator. I'm Irakli Beridze. A special AI center will be opened very shortly. I'll be heading that.

Now...let's get to the, let's get to this breakthrough session. Before I introduce the breakthrough session, I should make a short recap of what happened yesterday. This is wonderful. In the ages of the ITU, our convening of first global summit on AI. One of the main messages to me yesterday was the benefits of AI. We all have to capitalize on that and the potential of AI to contribute to the United Nations Sustainable Development Goals. We have to think about bringing together the risks of development and be mindful of maximizing the risks and minimizing the benefits. Certainly the key message and way forward that is proposed by the director and for many others, to create as intense as possible, international corporation.

Now going to this subject, of course, the issue of the privacy and security is one of the most important issues related to AI and recent developments, or recent occurrences of hackings and breeches of information is present. Never before, human kind has accumulated so much data and never before it was so easy or so easy to access this data and many devices which we use and later on we'll be using, will have potential to reveal our personal data. Therefore...and, once you add AI to it, obviously it's going to, the answer will become exponential as the technologies are growing exponentially.

Therefore...what we're going to discuss today and what is sort of most-important outcome of it should be that we need to identify the strategies to ensure that AI can contribute to the global peace and security and protect us from unauthorized manipulations and from creating, from creating chaos.

So...how this session is going to run, we'll have two, two lightning talked, right after my introduction and then we will have a panel and I will introduce the panel. And during all of these deliberations, and then, later on, obviously, we'll have questions and audience will have an opportunity to ask questions. At the end, our rapporteur is going to prepare certain principles which will come out of this.

So...our first speakers, not to go too much with my introduction is distinguished speaker from China. Mr. Hongjiang Zhang, I hope I pronounced your name correctly. Managing Director of the Bytedance Technical National Strategy Research Center. The floor is yours, Mr. Zhang, please come and give us your lightning talk.

>> Hongjiang Zhang: Distinguished guests, colleagues, friends, good morning. I thanked the panel chair for inviting me to this forum. I've learned so much in the past day and a half. So...today, I'd like to share some of my thoughts on the security and privacy issues. As many speakers so far, have pointed out, as AI technology developing and maturing, it has and will continue to bring in tremendous benefit to our society. Having worked on AI technology as a scientist, as well as a carbon exactive, I'm very excited to impact this wave of AI and what it will bring to us, the benefits and challenges are much stronger and wider than the past two waves in the past six plus years of AI history.

This is because...this AI wave is driven, mainly by new machine learning algorithms, big data and powerful computing resources.

However...it is equally clear that many of the AI applications we are developing could have the potential to compromise privacy and the security, adding to already worrisome capabilities, the connected device already brought in in our life.

Among all the potential issues, a particular one I'd like to address here is what do we need to do in the establishing and implementing new principles? And...data privacy and security in the world of AI.

It should be streamed forward to ensure that the data that AI is relying on is based on a combination of individual ownership. And...informed consent for its use.

Also...no human operator should have access to individual identity, similar to the personal property practice today we have already been using in some systems. In addition, given the power of AI abilities, especially in the event detection, AI, in fact, can be used as a powerful tool to assist us in identifying potential privacy breeches and use of data for criminal activities.

Therefore...I believe the key challenge is beyond technology. We should take on to rallying government, international bodies, and...privacy institutions to put a postured effort together to examine whether the current existing privacy and security standard and the regulations can still protect and safeguard personal data, individual privacy and, and our services overall and establish new ones.

Even the pace of innovation becomes more and more evident than often government agencies and international bodies are not as quick at private enterprises to react fast in the establishing and implementing standard.

This factor calls for, that private enterprises, big or signal, to show their social responsibility to cooperate, to lead in protecting privacy and security to win the trust about the customers and to ultimately unleash the full potential of AI technology.

Furthermore...leading Chinese provider in AI services, I'd add that another critical factor in driving administrations is to engage new players in the country. China in particular.

This could be an option, and essential part of our effort, if we want to make sure our effort is successful, especially to avoid potential [indiscernible] the technology could lead to.

When they have all known that China has become the world's largest mobile internet market. We may not have realized that China is rapidly developing into an AI powerhouse, driven by large volume of data, created every day by close to 1/3 of internet users. And perhaps the largest pattern base in AI technology.

The largest internet companies have all devoted tremendous resources into developing AI technology, but in my view, what's more refreshing is the new and successful outcomers who are exceeding the technology landscape.

So...as new industry leaders like Bytedance ourselves, those leaders are not necessarily known by the rest of the world. They are new generations of technology entrepreneurs and they are open minded and waiting to work with partners worldwide.

We need to engage them if we want to establish and implement new standard of regulations to be adopted, to adopt those regulations and understand them worldwide so that we can safeguard AI development to unleash the full benefit of AI technology that it could bring to our society. Thank you. [applause]

>> Irakli Beridze: Thank you very much, with time constraints, I'm introducing Virginia Dignum. She's an Associate Professor of TU Delft. She's Executive Director of the Delft Institute for Values and Global Initiative. With this, Virginia, please come and give your lightning talk.

>> Virginia Dignum: Good morning, everybody, it's a pleasure to be here. A lot of people, and the previous speaker, have talked about the need and necessity to ensuring privacy and safety in all AI endeavors. However, I wanted to take a bit of a profile position and ask you, is it possible to have too much privacy and have too much safety and what, what is the role of AI on ensuring that?

As you know, AI tends to be exaggerating on the defense it causes (?) Once you tell AI to create paper clips, it will create more and more until the whole world is covered in paper clips. It'd be the same on privacy that AI would go on and on and on, ensuring our privacy in a way that we wouldn't share any information with anyone, even if we would want that or need that. There are many cases, situations in which we do need to exchange privacy. And it is a change delta.

Safety, the world would become fully safe for us, I think that seems like innovation, like...very human property or

necessity of taking risks would be curtailed and that would probably not be a nice development for all of it.

So...the question I have is, what do we really want? What is really behind the issue of safety and privacy? Is just, just telling, developing systems to be private and safe and so on. Is that exactly what we want? Or are privacy and safety issues which contribute to our welfare and our well-being and should we take care of those more upstream or higher level view and making sure that systems are developed for well-being for good as we are discussing these days and take privacy and safety as some of the factors which can be taken into consideration for that overall good and overall well-being of systems.

So, I think that that's a different way of looking at privacy and safety which might give a more broader and more sustainable approach than just focusing strictly on privacy or safety. In fact...just recently in a book, it's referred to privacy as threats for democracy. The British PM has entered similar ideas in face of the London attacks last week, so...it might be that privacy, in itself, is not what we want or not always what we need to have.

So...I think that most sustainable approach is to empower all of us as users, as developers, as researchers, as society in general, to really take the responsibility and the awareness of what is there, behind the need for safety and for privacy. What are the real aims that we want to get with it? In a larger picture. And to take care that AI is developed in those higher values and higher aspects.

So, in a sense, I'd like to propose three principles for developing AI which would, in my idea, in our idea that we are working on, enable those, that possibility and those are, what we call the ART principles. Accountability. Systems are accountable, why do they decide to take this or that step? Why they have used this type of data for what? Why was that type of data needed and so on.

Responsibility in terms of use of stewardship. How are we managing and governing that data? Who has access to the data, who doesn't have access to the data. Create principles around the responsibility for good, sound, and valuable stewardship of data and other algorithms and so on.

And of course, transparency, being able to inspect or question about insights, verifying the functioning of those algorithms. I think that this type of principles are kind of broader and by taking care of looking at developing and using systems, responsibly, in terms of these principles, we can, we

are much more able to be using and considering privacy and safety in the global good and not as strictly as what we want to develop.

>> Irakli Beridze: Thank you very much, Virginia. Very interesting and of course, the proposals of responsibility and transparency. Something to take from your talk as well.

With this, let me introduce the wonderful panel we have. Very diversified panel. Geographically, very interesting from all over the world and all different backgrounds. I'll start from this point. Ms. Drudeisha Madhub, Frederike Kaltheuner, Mark Latonero, Brian Witten, and Konstantinos Karachalios.

With this, let's run through what we're going to do. We have prepared three sets of questions. And...I think the best way to do it would be to present the first set of questions with sample of questions. Each of the panel members will have an opportunity to comment and we'll go on with these questions. Of course, let's make it open and sort of interactive if at any moment somebody wants to have a follow-up question, we'll do it, but in the end, we'll reserve time for questions and answers from the audience as well and need to reserve some time for our rapporteur to present certain principles. I'll ask the panel members to be succinct and complete with their answers and remarks as well.

So...let's jump in with the questions. First set of questions would be about what are the key challenges in implementing current principles of data privacy and data protection in the world of AI?

And...for example, can we ensure that the data that AI has relied on is based on the recognition of individual ownership of the data and informed consent for users? And how can AI trust in the right to privacy by Member States, organizations, enterprises and citizens and for what, how can AI assist in identifying privacy opportunities and issues of data for criminal activity? So risk and benefit side itself as well.

So...I'll ask for a volunteer who would like to start commenting on that? Please?

>> Thank you very much, I think these are the most important questions related to privacy and security. I like the principle a lot. Enhancing privacy in a constructive way, the essential questions from a very legal perspective, they are legal points you just raised is how, actually, are we going to protect informed consent. In the world of AI, I don't see this happening at all. How can we actually see the consent of each and every individual involved in the world of AI. In practice

right now, we're having big difficulties in securing people's informed consent in every situation every day. I think this is something that we won't be able to achieve in world of AI, to start with. This is one of the main concerns I have and we have to devise a way for a new order, where AI will have to adapt to human rights, basic human rights principles, which will be sent in the world of AI. What we have right now is, we had the world of big data, we have many challenges in the world of big data that we're not being able to actually really counteract. We're having big challenges.

How are we going to really, you know, we don't have solutions right now, for these exists problems, so...what solutions do we wish to achieve in world of AI? This is the question and I don't have the answer, so, I'd like to give the other panelists a chance.

>> Irakli Beridze: Of course. With exponential growth, of course, this is the beginning, that's why ITU is having this organization and talking about this. Let's hear from the other panels, please?

>> Thank you very much. Given that the importance of privacy has been questioned. I just came back from a hearing on security at the Parliament. One of the main findings was that in a world where software and intelligence is embedded in the world and increasingly ubiquitous, security, privacy and safety challenges converge. And security is a common good that protects everybody. And I think there is a combination of privacy, security and safety that works to the benefit of everyone.

So, the reason why, a lot of times we talk about AI, we talk about things that are not yet there. Whereas, we, as an organization, have a term we call data exploitation. In the current world, a lot of individuals feel a complete loss of control over their data.

With a recent study in the U.S., 91% of Americans either agree or strongly agree that they've lost control over their data. And I think that shows that the current ways in which we protect privacy are being stretched or challenged. That being said, there are a couple good things to take from data protection regulation. One thing we like is privacy by design, a principle that often has security, data minimization, while AI relies on data, there are ways to use AI that preserves privacy without making sacrifices on accuracy, for instance.

However...there are three or let's say four main challenges that we see between AI and existing regulations and one is, I'm just mentioning, just adding this because it was mentioned. The

idea that data is an ownership, you have ownership of your data implies that your data can be sold. You have to be very careful that this doesn't mean that people with less resources, people who are poorer will have to trade in their privacy.

Data privacy is organized in the U.S. around the principle of personal data. Personally identifiable information. AI is challenging this concept. The entire idea of machine learning, to find patterns within data, there are privacy concerns that have nothing to do with personal data. If you think about detection software in public spaces, those kinds of problems are not covered by data protection laws.

The second one is, there's a blurring distinction between sensitive information and nonsensitive information in a world where you can refer people's personality, very private life from data that is publically accessible, sometimes, a lot of organizations are interested in and finally, knowing where to sync up and collaborate.

Also in Europe and data protections, the processing has been to be lawful, but also has to be fair and not discriminatory. If we make decisions about individuals or inferences where neither the designer nor regulators, nor the user can explain why the decision has to be made or the inference, it's very difficult for companies to comply with these principles of fairness and nondiscrimination.

>> Irakli Beridze: Thank you very much. Let's go to Mark.

>> Mark Latonero: The reason why I think privacy is such an important concern for all of us here is that it anchors this AI discussion in a fundamental human way. Privacy does ground the conversation in human rights, which I think is important. There is, you know, because of the raw material aspect of AI, there'll always be attention to AI, big data technology.

The questions are you know, what are the costs and benefits and balancing that and opportunities with risks and bonds and misuse. We're really going to have to think about the balance and the trade-offs. You know...what kind of cost is acceptable? Cost is an inherent aspect of AI, privacy is an inherent cost of an AI system.

You know...what is the reasonable balance of risk, of taking someone's private information with regard to what we're talking about at this conference.

What is the cost of not using AI due to privacy if there is a good outcome at the end of the road.

All these balancing acts and trade-offs is where the hard work is going to come.

You know...thinking through the thresholds within each community and practice, for when, for understanding this balance. You know...what are the red lines? You know, what types of issues and practices should we not collect by big data. What are the yellow sort of lights? What are the absolute green lights in that, in this context?

If I just, might add something else for now. We're going to talk about general principles, I think that's the right way to go. Transparency, incent dignity, responsibility, data minimization, et cetera.

Even in this AI world, some of these values become challenges, so...I certainly take the point and the provocation about you know, privacy, basically maybe being an impediment to AI for good.

However...this idea of solving that transparency might not be the answer when we say, friends that work in machine learning and networks, they cannot explain why the system has produced the result that was created.

So...it's, explainability might be an impossibility in the complex world we're building.

The last thing is that, once we do that, I think then the hard work is trying to apply those principles in specific contexts. You know...how might these AI principles work in the context of the humanitarian sector?

How might, for instance, in rapid response to a disaster. How might the principles may or may not work responding to something that happened ten years ago? You can go through every sector with, in the cases of experts to do that and see if these principles sort of apply. So...I'll sort of, I'll stop there.

>> Irakli Beridze: All right.

>> Mark Latonero: Thank you.

>> So, I want to start can informed consent. I agree with the sentiment that data is the fuel that drives part of artificial intelligence. I want to talk about how a lot of this data is collected through surveillance. Online, in compass websites, we now see the pop-up that says "do you accept cookies?" Cookies are just one of more than a dozen tracking techniques they use to not only track what you're doing on that site, but across all the sites you've ever visited and might visit in the future. That passes surveillance online, but as we move into the world of smart, connected physical Internet of

Things all around us, of countless cameras watching us, just as we walk down the street today, interrogating our mobile device, MyFi, location-based services. Knowing where we go and everything we do and listening to our conversations on our phones and smart televisions, added functionality and other home systems, technologies.

Everything we're doing, everyone anywhere near these technologies, trying to capture informed consent in that kind of world is, I think, extremely challenging to do and extremely easy to abuse. But...at the same time, I think it's a very important challenge to have. I like the provocative question that was mentioned earlier. Can we ever have maybe too much privacy? I'd say, looking over the course of the long arm of history, as long as tyrants walk the earth, they will sometimes come to power, even in democracies.

So, as long as tyrants walk the earth, no, you cannot have too much privacy. Technology is a valuable thing we see in artificial intelligence profiling people to serve them better with selective marketing, targeting attributes.

That targeting can be used, can be abused in dark ways. And might come to power in the future. These are very important questions to answer.

And at the same time, similar question, can you ever have too much security? We see proliferation of data everywhere to fuel AI. At the same time...in countless spaces, headlines continue to prove, security protecting those pools and lakes of data are often grossly inactive. That's something that might need to address this in society. I think there are lots of things the governments can do, lots of things that responsible companies can do. I think this will be an appreciation of the sensitivity of the data and the human interest here, doing this as well as, eventually protection for handling such powerful assets and data.

>> Irakli Beridze: Thank you so much. Now, Konstantinos, please, your thoughts on this issue?

>> Konstantinos Karachalios: Thank you very much. I want to say something about privacy and whether this is the focus. This is national perspective, privately, we don't get [too far from mic]. So...because this is private. Having said that, if we just get about the private affairs. There's another aspect of privacy. It is very important, the possibility to present ourselves the way we want to present ourselves. If you look at this, you are a political slave. This is where we are. They call it data feudalism. (?) We're going back to feudalism through technology.

The question is, what is the purpose of this technology? What is the purpose of artificial intelligence? Just before, within the last Plenary session, this guy with the rapporteur, asked what is the purpose of it? They couldn't answer it. We're doing it because others are doing it. But they didn't answer the question.

What are we talking about? What is the problem we're trying to solve? I'd make it even more explicit, if a technology or everything we're doing is not promoting our autonomy as humans, if it doesn't promote political autonomy then it is useless. (?)

So, suppose this is the question. Why are we doing this? If something doesn't make sense, the technologies and science, at least our duty assigned in these technologies to question what we're doing. We've started with different organizations, we've established a good program, take into account the design of AI and so on. The question is what, because...in terms of logic of the companies, you want to make your money, you don't care about the rest, most of them, the governments, perhaps the governments are unethical? You can see [too far from mic]. I don't understand this. We must decide what we want specifically.

Then, people like you here, the Civil Society, human rights or political autonomy, just get rid of it. This is what we're doing at IEEE and we cannot ignore it anymore. First, we must decide what we're doing. We're a driving force, per se.

This is very complex matter.

>> Irakli Beridze: Thank you. Let's, let's give the opportunity to Sean to comment on that and then we need to move on to other sets of questions.

>> Sean McGregor: I'm hearing a tremendous amount of debate on general principles we'd like to examine the issues of security. One of the goals of mine is to try and drive these principles into guidelines that are actionable, which may be difficult since we're still trying to get to the root of the question and...what we'd like to achieve, but...we're able to, in the course of the discussion, drive towards some consensus and, or even process that we can drive forward in the future towards greater consensus. Particularly since we're here in the UN and trying to drive these principles forward. So, I'd just encourage the discussions to move towards something that's actionable where possible.

>> Irakli Beridze: It's important to understand the issue of end routes, which we're discussing. Virginia and Mr. Hongjiang, if you'd like to give your insight?

>> Virginia Dignum: The data's full. If we take the technology, fuel efficiency is very important concept. I've been working in AI for 13 years. At this moment, AI research and development, we have too much data. We have too much computer power, so we can just use algorithms and systems that we have so far and take those as they are and say "okay, sorry, the algorithms don't allow for inspection, sorry, you can't do anything about it".

But AI is technique, something that we develop. As AI research, and I think I would welcome more constraints, constraints in terms of regulations. You can only use so much data and then let's go find algorithms, the issue of too much, huge amount of data, and also issues, regulations concerning inspectability and transparency of algorithms. Other algorithms are more amenable for inspection. We don't really have to stay with the algorithms of the systems as they are now.

So...regulations and constraints is something I think will benefit and drive forward development of AI.

>> Irakli Beridze: Okay, Mr. Zhang?

>> Hongjiang Zhang: A lot of the perception and variety, when you install an app on your phone, there's a privacy alarm, so you accept this application, you choose those options. If you choose those options, we need to ensure those companies come up with those apps, make it very clear, easy to understand that you are participating in, by giving up your privacy of contributing data, but your data will be used. Those products have been there, personalized advertising, targeted advertising have been in practice.

So...I should, I want to make sure, we shouldn't overstate it.

Another thing is expandability. Actually, if we look at our history of our brand, how intelligence develops. A lot of decisions we couldn't make. If you like [indiscernible], could you really, mathematically, you know, expandible fashion to say why I like it this way. Why it has to be this way to be appreciated. No, this is our human intelligence development. We cannot expand our own decision, how can we expect a machine to do that?

So, algorithms encourage us. There are challenges, living more [indiscernible] than humans. (?) No problem. The last point on this, your point, too much data, in the world, there's never a term of too much data. You want to cover the entire space, you have to have that much data to cover the entire space.

In the early days of scientific discovery, ever since experimental in the sense that you observe, you observe how many stars. Try to figure out their relations, then come to physics, then you start filling models. Then six years ago, you start using combination of models as computers are powerful. Weather systems, today, we come to the fourth paradigm. Data-driven. Data-driven paradigms. This is actually how scientific research progressed in the last 2,000 years. And you have this much data and data from our scientific research, data from our experiment, data from our life. Uses of data is few. Taking care of the privacy issues and security issues. But...our life relies on data.

>> Irakli Beridze: Okay, thank you for the reflections and insights. We have to move on to the next set of questions. If we ask questions of, how can AI better protect the human rights? Okay, so...if we can do a very quick question? Then we need to cover other sets and then we will have question-and-answer session as well.

>> Hello, I wanted to add some concrete points. What Sean was saying, we need to move from the abstract, right? To Virginia's point, she talks about data, looking at fuel efficiency, right (?) There are techniques and gaps, generative, actually, they have proven to be quite effective in generating synthetic data which can then subsequently be used for training. That's one concrete way where you can start to limit the use of too much data, right? To jury point.

Additionally, there are techniques and you're from Symantec, maybe you can corroborate on this. There are techniques called encryption. They yield the same results as things you'd get as operations on Kleenex (?) Applications that train on using the more technical principles could be one concrete way of going about it. I don't know, as a panelist, you see these are techniques that are being taken up by policymakers.

>> Irakli Beridze: Shall we just take a question or comment? We'll have other questions to cover as well and we have 14 minutes left. Please....

>> Richard Hill: I wanted to make two concrete suggestions. The first regarding data, it seems to me, the concrete step is to call for a model law on the data privacy and protection and encourage all states to implement that model law nationally.

The second point I want to comment on is security, which we haven't talked about yet. It's not directly related to AI, but it is indirectly. Some of you have heard that Microsoft has proposed a Digital Geneva Convention. It's basically asking

states to refrain from attacking civilian infrastructure, but also taking a positive step of disclosing any abilities they become aware of. I'd propose it's not this group that we support Microsoft's initiative.

>> Irakli Beridze: Thank you for your suggestion. One more and then we're moving on.

>> One thing, just around how we're talking about kind of the, the kind of things that have been done to affect privacy now. For example...the notice that you get in EU about cookies. Which...I'm sure has good intentions, but it's completely useless. It's completely empowering. It's on every single website. If we end up with things like that with AI, it looks good, seems like we've done something, but it doesn't do anything for anyone.

>> Irakli Beridze: All right -- I have to move on to the other questions and then we'll have reserved time for the audience to comment as well.

What we, also, sort of agreed to, to discuss here is that, how can AI better protect the human rights in the algorithmic age. I'll encourage some of you who feel comfortable to answer it. Please, Drudeisha?

>> Drudeisha Madhub: This is a question everybody should reflect on. If we could, actually, as a solution, technical experts probably know the answer to this, how to invent human rights, values and principles into these technologies. We are talking about data philanthropy and other such things. How are we going to do that? If there's a solution to this, then I'd be very happy, thank you.

>> Irakli Beridze: Right. I think this is a question that Konstantinos wanted to reflect on that.

>> We have precisely a good working [indiscernible] of this question. [Too far from mic]. Groups of experts working on human rights precisely. Subsystems in human rights, we can talk about the rest.

>> Irakli Beridze: Yes, this is very important work that this group does and fully support such activities and part of the initiative as well. Virginia, please?

>> Virginia Dignum: I don't so robots getting rights. They're artifacts.

>> Irakli Beridze: Anyone else? Mark?

>> Mark Latonero: Bringing together human rights and domains of various human rights. Bringing into the conversation scientists and robots, these two worlds don't necessarily talk to each other. Even the corporate world doesn't talk to human rights all the time either. I think there's a long translation-type of process with these groups getting to understand the language and values and systems of thought that

we're dealing with. So...I think in terms of processing, that's right on.

One other point, which is, you know, how AI can be used to enhance human rights. I think there's a huge upside in potential for, like everything I said about big data collection and AI, the use of AI to sort of fine-signal human rights, potentially, even, in an early warning, sort of advanced early warning system, which potentially can predict when conflict may be occurring or may be occurring in the future. I think the trade-off with that is harder, that would require data sensors, massive data collection and the trick is not to essentially build a greater surveillance system than we already have in human rights.

>> Irakli Beridze: Thank you, Mark. Certainly there's a huge potential for AI contributing and better approval base. Frederike?

>> Frederike Kaltheuner: Traveling a little bit, I noticed around the world, as information technologies rises, everyone is doing better, it's easier for everyone to respect each other's human rights a lot easier. One thing to not lose sight of, as AI allows us to make the world better for everyone, whether it's through robots or the example that's personal to me, we all depend so much on these infrastructures. Allows everyone to more easily respect everyone's human rights. And we actually use AI to protect that. We use AI to process [indiscernible] every month.

Given that we depend on these infrastructures, technologies like AI, I don't want to lose sight of how that enables us to lift people out of poverty. How we improve quality of life and more freedom.

>> Irakli Beridze: Thank you, for this insight. Anyone else want to comment from the panel?

>> To address the point that it cannot be day time science, data that is used to generate knowledge about individuals, make decisions about people or make decisions that significantly affect people. I'd like to highlight that the United Nations Human Rights Council this year, automated policy, the idea of contributing to the initiative, I think it's very important. The idea to adapt human right into AI technology is very challenging. And...the second point I wanted to make, we talk about AI in the abstract. Anything from robots, machine learning for targeted advertisements, autonomous weapons, so...there's very different levels of abstraction. Human rights concerns are domain specific and we cannot come up with universal principles that apply.

>> Irakli Beridze: Right, it's a huge issue. Anyone from

the robotics strike activists? Okay, please....

>> Robot stuff is interesting. To start from the basics, first of all, where does wealth come from? Wealth comes from quality of life of people. And...so, where does quality of life come from? You want to avoid totalitarian states, dystopias, 1984 kind of thing. And dystopias come from universal surveillance. This is sort of an east Germany kind of thing. It's not just, it depresses the economy, it depresses the spirit of people and depresses the quality of life. There's less wealth in the country. There's, there's, less economy going on.

One of the key problems that we have right now is NASA surveillance. The governments have decided that they're going to step in and even if you say that you're going to protect the data, they said, we're going to force you to give up the data. And...because the governments are much larger than the people, and...there's a trade-off between security and actually privacy.

So...I'd suggest, as an actionable item, that possibly, privacy is a human right, so that's a question that we should debate. And...if it's a human right, then maybe end-to-end privacy encryption for individuals is an international basic right of the people. That they should have.

And...if you, if we can turn that around to make the government's be transparent so that the people can, can monitor the governments, then it's going to be a lot easier to make sure the governments don't run away.

>> Thank you so much for the comment. I take one or two more comments --

>> Avoid totalitarianism.

>> Just quick comment on data. I think we have to think about data as a reenergy and not a new oil. We can recycle and use for many different purposes. That's one thing. The other concept that we haven't touched, exactly is group privacy. Which, being practical with AI is a critical concept. At the end, AI creates a statistical output, many times we don't know what the machine is doing, but typically targeting a group of users. Here, the question is, shall we have a specific recommendation, a specific rule that deals with group privacy?

>> Irakli Beridze: Thank you very much, one more and then we'll have more time later.

>> Just real quick, Facebook is working with China to try and monitor everybody to make sort of, a yelp for people which will affect their credit rating and whether they're advanced in government and allowed to have housing or not. That's something to think about it.

>> I'm from the World Health Organization, just hearing a

lot of this discussion, the question is, it seems like we are asking for some standards and guidelines and definitions of words and phrases and terms in relation to what is, in this context, what does privacy mean? In this context, what does human rights mean, et cetera. The question is, because this is so global, which sort of organization or, or what, what, I suppose, organization can, or should take responsibility for developing these standards which everyone could agree. The second question, in relation to that is [no sound] -- what sort of safeguards AI applications. I got down the data collection method, et cetera. Have respected privacy of people and human rights, et cetera. Seeking approval, in a way.

>> Irakli Beridze: I think that we are at the stage when we're discussing the basics at the moment, still and we have far way to go before there'll be any kind of UN charter or convention or an organization created which will deal with these issues.

Of course, the issue is very broad and there'll be many different types of sets of issues which would be dealt with by different kind of international organizations, therefore, I think we are not there yet. We'd be talking about a real set of regulations and giving a mandate to a particular organization which would do it. Certainly, we heard yesterday, the Secretary-General was very interested in these issues. As far as AI development is concerned and sort of coming up with very interesting suggestions of creating task forces and committees and Secretary-General was very interested in taking some portion of leadership there as well. So...therefore, there are still preparatory works happening there.

We'll take just one more comment and then we need to ask another set of questions and then we'll have the audience also, please...sorry, I didn't mean to ignore you.

>> I'm from the IEC International Technical Commission. There's not going to be a single organization that will develop. I think there are organizations that are already in this space of developing international standards for all kinds of states. The IEC, for example, develops things in Health Care, but also in automation. ICITU, there'll be a lot of people that will be collaborating in this space with lots of different facets.

>> Irakli Beridze: Absolutely. Hopefully the ships will turn into a fleet and we'll come up with good results. I need to move on to the other questions, relating to peace and security. Will peace and security be enhanced or compromised with advancements of AI technologies? And for example, are we ready for a sophisticated AI-related technology to deliver weapons by hacking into drones or self-driving cars, bigger

networks and in combination with explosive materials, chemical, biological, nuclear weapons and materials? And how, at the same time, can AI technology help to navigate these terrorist attacks? This is a big issue today. When you add explanations of sophistication to it, many questions would arise and certainly, I'd like to kind of, also, very briefly to comment on that and what we should be doing about it. Who would like to volunteer on that? Please?

>> Drudeisha Madhub: Let's say not legal measures, but technical, to start with, technical measures and safeguards that each country can actually take to really, in the short-term, make sure that there is no proliferation of black market weaponry.

>> Irakli Beridze: Right. Anything could be used as a weapon and that was the sort of idea that how --

>> Drudeisha Madhub: AI used as a form, are we not contributing to new form of terrorism? Which is not actually you know, which, another way to look at things. That's what I want to know. If, let's say, terrorists actually use these technologies in the wrong sense, we are actually contributing to a new and more dangerous way of terrorism.

>> Hongjiang Zhang: AI is a technology, doing certain things, you apply it to medicine, and beneficial things it's really, you know, we should really be looking at applications, particular applications of AI technology. It's not AI itself. AI is enabling. It's like water. Water can keep us healthy and it can also flood our houses. So, there's nothing wrong with the water itself.

AI is an enabler. Will AI kill people? That's not the point. If you use it enough to enhance what already existed, that won't kill people. I think in this sense, we attach too much stuff to AI and it's just an enabler. We need to make clear of it.

>> Virginia Dignum: I agree with you. We're going to use AI for good or bad. That's as for any other technology. You can always come up with applications which would be good, applications which would be bad. And the issue is more like, how are we going to really take responsibility and empower other ones to also take that responsibility and the use of the technology as any other technology to use it in a responsible and beneficial way. It's not AI itself.

>> Irakli Beridze: Frederike, you want to comment? Oh, Mark?

>> Mark Latonero: We're entering into a long-standing debate about the nature of technology. I'll quote one person, Melvin Kransberg said technology is no more good than bad than mutual. (?) Values, biases and other types of social concerns,

such that you know, technology isn't completely mutual.

>> Frederike Kaltheuner: Unfortunately, it's been demonstrated that millions of cars can get hacked, you know, very straightforward, even without artificial intelligence. It's relatively straightforward. At the same time...attackers are leveraging artificial intelligence. This is rapidly an arm's race between various attackers. As we think about the physical world, one of the things to realize, we think about drones, the barriers the crosses entry with drones over the last number of years has gone down from millions of dollars to hundreds of dollars. It's sort of a fundamentally different era we live in and we're coming into. Protecting and mitigating against smart technology, you can take down an aircraft with hundreds of people on board.

At the same time...I'm sort of aghast at the number of technologists that I engaged that really aren't even thinking yet. About the moral and ethical aspects of what they're doing and how it could play out.

There are a lot of people advocating for law and regulation and other solutions. Those might or might not be powerful levers for solving this problem.

One of the levers we need to introduce here, hippocratic oath and introducing around computer science curricula, more training on that, more education and there's a great talk out there if you haven't seen it yet. The Ted talk and it contrasts sort of the merits, the moral Operating System, the next great thing, as opposed to a mobile Operating System.

>> Irakli Beridze: Thank you for that insight. Konstantinos?

>> Konstantinos Karachalios: It's our responsibility. We can't just work on the political class. The problems we create. So...when we work on design systems, we must be talking about the consequences. It's not easy. Each program is used in different way, without this, we're going to know the problems we're creating. And to come back to this question, I think, I'm not so sure [indiscernible] [too far from mic]. I see computers, I see data. I see the issues. But what I see more is the steps we've found, sensors. We are going into something [indiscernible]. It's a different democracy.

So...for me, I think a space without sensors, what you see [too far from mic]. This is my personal take.

>> Irakli Beridze: Great.

>> When we talk about objectives and things, of course, sometimes it can be that AI is not appropriate to use in certain circumstances. What is interesting about this, so...according

to the documents, obviously, what is interesting about this is that you can also use machine learning for targeted advertisements. And a very, very low margin of error that would be impossible to reach in such a thing as advertisement would mean that ten thousands of people on these classifieds can have severe human rights implications. If we use machine learning to classify people, there'll always be a margin of error. We should seriously ask ourselves whether there are domains where we simply should not rely on such uncertain knowledge.

>> Irakli Beridze: --

>> I'll put my hand up and say -- [indiscernible]...that has absolutely nothing to do with behavior. Please don't ever kid yourself into believing [indiscernible]. Look at any country and how this works. Humans are very different. Please don't think that's what -- we have to rethink what it really means. To me, the real thing, there's information symmetry. Society going forward will be another market. We, as a society need to understand what previously less society means for Health Care, for everything, that's something that we haven't thought of. Somebody mentioned encryption, used to be a researcher. We need to understand -- we have a toolset of things we can apply to, for example, computing, some parts of it. You can actually prove you can have things and things are being run the right way. There are whole toolsets not being used.

>> I worry that encryption isn't needed and say the security isn't evaluated the same as advanced encryption standards. At the same time, there are a lot of people mentioning homomorphic encryption. A very dangerous way of thinking. The other technologies you mentioned, in contrast, like...various forms of trust computing, are relatively mature and relatively underutilized today for protecting lots of information in lots of places.

>> Irakli Beridze: Now the floor is open and people can comment. We have five minutes for this.

>> Can I have one more quick comment? One thing you should notice, security analytics, the thing you described and recognize, there are a bunch of people that provide software [indiscernible] as an example. In the case you described, the travel pattern very close. There are huge intelligence, it's very, very hard to apply mission learning to security analytics. It's ability detection. When you're looking for that, if you make an error, you're pretty much given a death sentence. That is never factored into --

>> Irakli Beridze: Some of the discussion can continue during the coffee break as well. I understand this is a big issue, very diverse.

>> Thank you very much. Can you hear me? All right...can

you hear me? All right...so maybe, [feedback]. Good now? My business is terrorism and law (?) I'm always looking at the bad nature of human beings and I'm joining you when you say about, when we're talking about terrorism, my question is, how do you control open source information and data when it is out because we always find people to contribute to systems (?) Cultures being used by ISIS. They're weaponized with grenades and she'll. We are in infancy of this technology. What if this technology, and it will fall into the hands of bad guys, how do you control that? How can you mitigate this problem?

>> Yep....

>> The....

>> Can I just --

>> Irakli Beridze: You wanted to comment? Please.

>> Virginia Dignum: I think that's one of the comments mentioned a few times. AI is a technology, again. It's not something which we should allow or address to work on itself. It's collaboration between the AI systems and the possibilities of AI in general. And the people, the issue of the human control in the group. Something we have to stress much more in all the principles of sustainable and responsible use of AI. We don't allow systems to take the decisions worldwide and there are always, they should always be some humans in the group which impact the responsibility.

>> Irakli Beridze: We'll take a couple more comments. Please be succinct. We have only ten minutes left. I was given an hour and a half to run this session.

>> Thank you so much. I would first of all like to refer to Brian of Symantec, the active stage of cybercrime is by itself. Looking of course, into the future, in the third limelight, you don't have ton an expert anymore to contract services to execute.

The second concern which I've heard today is basically security in the private security, away from the public sector. In the past, public sector, of course, was the first responsible entity to deal for the protection of its constituencies. That's not normally the case.

The third one I'd like to refer, we just had an intergovernmental expert group meeting in Vienna in April. It is still close, very difficult discussion. So...let's be real on what we can do. The political reality is still very important.

>> Irakli Beridze: Certainly we need to take all of this into consideration. Please?

>> UNESCO Commission is currently looking, producing a study on ethics of robotics. I want to make two comments.

One...in the application, the way in which we need to look at the ethics of the use of these systems is, I think, very much the main specific. We can't produce generalizations on things like accountability, responsibility, et cetera.

I'd like to make a comment on the weapons issue. First, I'm pleased to hear many comments, both, one just now from Virginia and also this morning, there should always be a human in the loop. There'll always be mistakes. There are recognition problems for weapons. The system cannot distinguish between an umbrella and a gun. (?) It's not just, we need to look at how the bad guys are using these systems, we need to look at how the good guys, if you wish to use that terminology are using these systems. We need to have some, some regulation, if you like, for how we're developing AI-related weapon systems. And...this is an issue which I think we need to give a lot of attention to.

>> Irakli Beridze: Very quick comments, please.

>> Hi, I'm Zoltan, formerly Chief Strategy Officer in the government. Invariably, it's a good thing. This conference is talking a lot about that. It makes sense, but...when you talk about legal systems, you have to talk about how to enforce them, what are the sanctions, if they're broken and who will be playing that role? I think it fundamentally raises a linked question about oversight. What is the oversight that needs to be placed around this entire debate and agendas and who will be doing that? The global financial system, for example, all the good and bad things in it is complex and it has a global supervisory system which actually, sovereign governments linked into. You need to find a responsible government that says we need to call for a global supervisory system. Maybe you should do it in a form they're comfortable with. The financial consequences of having to enforce laws that can't work is important. Take it to G7, take it to G-20. Get a sponsor government to say we need to debate this, but we need to think about it in a rational way. The national political engagement is maybe the first practical step around thinking about this.

>> Irakli Beridze: Thank you very much for your comment. Obviously the question would be when and how is this going to happen? When is the right time and whether we really understand the issue if we want to take this on or not. I mean, we don't have time, unfortunately for more questions, I apologize for anyone that didn't get an opportunity to ask a question. We have now time for Sean, our rapporteur to give us some of these insights he took from this session and then we will thank our panel afterwards.

>> Sean McGregor: Thank you for all the contributions, I'll do my best to distill this into something that's actionable

and to go on the last comment from the audience, the first guideline or recommendation that I think would be largely universal for this room would be to assign, identify or convene a world governance body to lead or coordinate on security or privacy issues. Bringing in many stakeholders that exist and having different areas of expertise and to drive towards international consensus.

One of the things they'd be able to do for existing bodies, would be able to do in developing action or way forward is to create model laws concerning security and privacy, encouraging countries to adopt those separately, so that's, essentially, creating more formal, legal guidelines to be adopted. One that came up, that I'm not as familiar with, but I plan on looking up after the session. Someone brought up the Digital Geneva Convention. I'll research that before producing the full set of guidelines. Finally, something that came up, some technologies for solving these problems technologically, we could invest in win-wins that enable privacy and security White House reducing the strengths of the eye and those would include strategic investments in the research of subfields of, this one didn't come up, I don't think. But multiparty computation and so forth. So, I plan on writing these up, circulating them among the panel and I believe there'll be an opportunity for input in the Plenary sessions, regarding how people feel.

>> Irakli Beridze: Thank you, you did a fantastic job. This isn't the final version, you'll write it up and there'll be a Plenary session when this will be presented. You'll have an opportunity to further comment on it. Any last words from the panel? If not...let's give a round of applause to all the panel members.

[applause]

>> Irakli Beridze: Did you want to say something?

>> This discussion was valuable to me. The evil isn't in the knife, but how it's used. It's not the millions of people that cut their dinner every night, it's the one crook. Maybe it's not oil, maybe it's not green energy, but data power. One of the solutions that just occurred to me, where companies pull that much data together, it's dangerous to democracy, should data collection be passed? We can't regulate the way we're doing it.

>> Irakli Beridze: With this final comment, first of all, thank you for your attention. I'd like to thank our panel members for their fantastic contribution. I'd like to thanks of course, ITU for organized this event and finally, I want to thank our colleagues who actually helped to shape this session and this is global policy and high commission for human rights. Please give them round of applause for their fantastic job to do

it. Thank you for your attention.
[applause]

[Presentation concluded at 5:01 a.m. CT].

****

****