OPEN SOCIETY FOUNDATIONS

TRANSCRIPT

"SURVEILLANCE, PRIVACY, AND FREEDOM OF EXPRESSION"

A Conversation With Alexander Abdo, Frank LaRue, and Katitza Rodriguez

Moderator: Philip Alston

* * *TRANSCRIBER'S NOTE: unfamiliar names spelled phonetically.* * *

ANNOUNCER:

You are listening to a recording of the Open Society Foundations, working to build vibrant and tolerant democracies worldwide. Visit us at OpenSocietyFoundations.org.

PHILIP ALSTON:

My name is-- Philip Alston. I'm one of the directors of the NYU Center for Human Rights and Global Justice. It's a great pleasure to welcome all of you here tonight. We have a-- security, and perhaps also freedom of expression, obsession at present.

As many of you'll know, our center just launched a new blog, which is called Just Security. I hope you get the pun there. It's www dot just security, one word, dot org. I would encourage you to look at that. We had a major panel in Washington, D.C. yesterday-- organized by my colleague here, Ryan Goodman, who is really the key person in setting up the blog-- and co-directed with Steve Vladeck from American University.

Tonight-- I wanna begin by saying thanks to the Open Society Fund, Sandy Coliver in particular and her colleagues, for having been instrumental in helping us to get this panel together. To my colleagues, Veren Ockehaffen over there, who's the director of the Center for Human Rights and Global Justice. To Audrey Whatney, who's probably not here because she's still working, as she always does. Thank you.

I won't waste any more of your time with me. We plan to ask each of the three

panelists to speak for 10 minutes. I plan to be ruthless and authoritarian in the-- (FEMALE VOICE: UNINTEL)

PHILIP ALSTON:

--old human rights tradition-- (LAUGHTER) in order to enable us to have time for a panel discussion-- and for questions. I hope we can really engage on this. No topics could be more-- timely than the ones that we are about to-- explore today.

So the-- the speakers-- I'll introduce each of them. I think perhaps in order, in fact at the time. So the first speaker and is Alex-- Abdo, who is a staff attorney for the ACLU National Security Project. I should say just in case there was any-- Alex, sorry to interrupt your introduction, because in case there's any grave disappointment, we had-- arranged for Robert Litt, who is the-- senior legal counsel to the director of National Intelligence to be speaking today.

The-- I think he-- that was deliberately undermined by Senator Feinstein, who-- (LAUGHTER) chose to schedule a hearing at exactly the same time just to screw up our meeting. And so Robert Lipp had to withdraw, unfortunately. But Alex very kindly came in to present what be a marginally different perspective (LAUGHTER) (UNINTEL) on the issues.

Alex-- is counsel in the ACLU's-- lawsuit challenging the activities of the N.S.A. He's been involved in litigating the Patriot Act, the-- the FISA, the International Emergence of Economic Powers Act and the treatment of detainees in Guantanamo. Suffice it to say that he's-- a bona fide pain in the neck from the government's perspective. So it's-- a great pleasure to welcome him here tonight and to hear his-- views on the current state of the-- the art (?). Alex?

ALEX ABDO:

Thanks so much for having me. It's an honor to be here. I had debated-- as a fill in for Bob Litt to-- to give you five things I would have done as Bob Litt-- (LAUGHTER) in the National Security Agency, but I'll spare you my wish list. So I-- I've been tasked with-- giving a broad overview of what we've learned since June 5th of 2013, which is when Edward Snowden-- shocked the world with the disclosures-- from the N.S.A.'s-- most hidden files.

And I'll start very broadly and I-- and then I'll try to cover what I think-- is a path forward. What-- what the problems are with the disclosures and what the way is to-- solve some of the problems. And-- very simply we've learned in the last few months that there's virtually no technical limit to the N.S.A.'s capabilities to sweep up-- communications, domestic or international. And there are few meaningful legal restrictions on the N.S.A.'s authorities-- to use those technical capabilities.

Today we know that most of the N.S.A.'s surveillance authorities take one of two

forms. The N.S.A. engages in the dragnet collection of so called metadata. That is information about our communications. For our phone calls, the N.S.A. now collects, we know, a record every single day of who we call, when we call them and for how long we spoke-- in addition to some other information. We know that until 2011 the N.S.A. did the same or essentially all emails, including all domestic emails. Who we emailed, when we emailed, how often we emailed.

And we know that the N.S.A. has other bulk collection programs that we don't know about. We suspect that some of them pertain to location information. Senator Wyden-- who's a bit of an oracle in this area-- has a habit of asking the N.S.A. questions that they deny and at the end of the day turn out to be true. And just today he-- once again asked-- DNI Clapper, "Does the N.S.A. collect location information in bulk?" And the response was, "Not under this program." (LAUGHTER) We don't know which program it is.

So that's the-- the bulk collection that the N.S.A. does, of even Americans'-- information. About every one of our communications. It happens on an ongoing daily basis. It happens today and it happens to you. If you picked up a call-- today or if you made one, the N.S.A. will soon have a record of it, if they don't already.

The other form of surveillance that the N.S.A. engages in-- is in the content of our communications. The rules here are-- a tad trickier-- but they're really-- a bit beside the point, because the rules are, at the end of the day, quite weak and subject to a number of exceptions-- that essentially give the N.S.A. carte blanche to listen in on any-- of Americans' international communications.

If you call someone internationally, if you email someone internationally or if you are someone-- who resides abroad, every one of your phone calls and emails can be the subject of N.S.A. surveillance. And that's a consequence of the-- extraordinarily permissive rules that the N.S.A. has. Rules that were put in place in 2008.

If you remember in 2005-- *The New York Times* revealed that the N.S.A. was engaging in-- widespread and warrantless interception of Americans' communications. And Congress responded to those revelations not as you might expect, by putting in place new measures to protect Americans' communications from warrantless surveillance, but by ratifying the program and, in many ways, expanding it with the law that was passed in 2008.

Today there are two primary restrictions on the N.S.A.'s ability to sweep up-- Americans' communications. One is that the N.S.A. has to be targeting a foreigner. It turns out to be a very permissive restriction, because the N.S.A. will presume you're a foreigner if you reside outside the United States-- and they have no information to the contrary about your citizenship.

And the second restriction is that-- they be trying to gather foreign intelligence-- which is an extremely capacious term. It doesn't just mean information about terrorism. It means information about the foreign affairs. If you're a human rights researcher-- talking to a journalist in Syria about the conditions on the ground, you are communicating foreign intelligence and your communications with the human

rights in Syria are very much fair game for the N.S.A.

And it turns out that the rules are even more permissive than that. The N.S.A. will presume that you are communicating foreign intelligence if you're talking to a foreign. Or, if your name, phone number or email address appears in a contact book of a foreigner.

And at the end of the day, these rules-- might to essentially carte blanche for the N.S.A.-- to listen to foreigners' communications, even when they're communicating with Americans. And the rules on determining citizenship are so permissive-- that in the course of that nominally international surveillance the N.S.A. also sweeps up, we now know, tens of thousands of even purely domestic calls.

And when those calls and emails are swept up, the N.S.A.'s rules don't require them to-- purge those emails or calls from their files. They can keep them for up to five years. And if they contain information about the foreign affairs or information about crime, or if they're encrypted, if, for example, you're trying to protect the sensitivity of your communications, then the N.S.A. can keep them indefinitely.

So those, very broadly speaking-- are the programs that we've learned about. And that's where the prison program fits in. That's where the upstream collection program fits in. And this where the Verizon program fits in. Those are the programs-- that we've learned about.

And they're problematic for-- you know, I think a number of reasons. The N.S.A.'s and the government's primary defense of its dragnet collection of our metadata, information about our communications, is that metadata is just metadata. It's not the content of our communications. And I think that's a myopic view-- of privacy in the new world, particularly when the government increasingly relies on the sophisticated technology-- of big data to analyze our associations. To create-- enormous graphs of who we communicate-- with, when and how often.

How those relationships change over time. Whether we call one person at 2:00 in the morning or another at 10:00 in the morning. That information can be extraordinarily sensitive. And particularly when it's aggregated-- over long periods of time. It can often give a more detailed picture about your communications and your associations than even the content of your calls and the content of your emails.

That's in part true, because content is deceptive. People can write in code. People can write with hidden meaning. People can write in different languages, in ways that-- may not be easy to decipher for an N.S.A. analyst. But your metadata, the information about whom you're calling, whom you're emailing-- is very difficult-- to obscure-- from those who want to surveil your communications.

At the same time we've learned that the structural protections-- the protections that are supposed to-- prevent these laws, these extraordinarily permissive laws, from going beyond even the bounds-- that they set out, have failed.

The Foreign Intelligence Surveillance Court, which is the secret court that meets in Washington, D.C.-- that's supposed to put a check on the N.S.A.'s surveillance

practices-- has shifted its role-- in the 35 years since it was created. In 1978 it was really-- created as a court designed to approve individualized surveillance applications. And it was designed to make very simple factual determinations. Is the government's target a legitimate target of surveillance?

Today that court-- we know, at the urging of the government in the years after 9/11, issues opinions of extraordinarily broad legal significance-- that affect the right to privacy of millions of Americans, interpreting what the Constitution-- requires and what our laws need, entirely in secret in a way that thwarts meaningful public oversight, that prevents debate in Congress as to the wisdom and legality-- of these programs, and also-- prevents public judicial review of these programs-- by courts that might oversee them-- including the courts of appeals-- or the Supreme Court.

We also have learned that-- the n-- that the FISA court-- troubled as it is already by being asked to litigate the meaning of our laws in secret also has to rely on the representations of the government. And we know now that the government has repeatedly misled the FISA court-- in secret filings.

That for years programs operated-- in violation of even the very permissive-- laws that Congress had set out. And that those violations persisted precisely because the proceedings in front of the court-- were secret and only the government appeared. There was no other advocate before the court to push the case of civil liberties. To argue that the laws had gone too far. To argue that-- they were unconstitutional as passed. And that has had a dramatic consequence-- for the work of the court.

Congress, for its part, has also been an inadequate check on the N.S.A. surveillance authority. It has also been-- kept in the dark, largely by the N.S.A. secrecy. Even the intelligence committees, who are supposed to oversee-- these activities, can't have the type of meaningful debate that might benefit these programs because they're prevented from talking-- generally with their colleagues outside of the committees, unless they meet under extraordinarily closed circumstances.

We know as a practical matter that it doesn't happen. And we know as a practical matter that most of Congress didn't know how the government was interpreting these laws-- when-- when they voted to reauthorize them repeatedly over the past few years.

And finally-- the public has been kept out of the debate entirely. Organizations like-- the Electronic Frontier Foundation and the ACLU and others have pushed for-- the last 10 years really to understand how these surveillance authorities are being used, how the government interprets them-- to no avail. The government has, at every turn, argued that releasing even a word of the government's secret interpretations of law would compromise the national security. And we haven't had a robust public debate. We haven't been presented with the government's affirmative case-- and we haven't learned about the widespread abuses that we've now learned about.

Those are the problems. I'll very briefly say-- that there is a path forward. You know, there are a number of I think very concrete steps that-- Congress could take to end unlawful surveillance and put us on a path toward the type of surveillance the N.S.A.

should be engaging in.

Congress should end bulk collection-- of our metadata. When it has a reason to spy on an American it should go to a court and obtain authorization to do so. Congress should also change the way that our international surveillance works. It should build in better protections for Americans and it should begin to have a conversation about the right to privacy internationally.

Privacy is not just a civil right. It's a human right. That conversation has not happened to a significant degree in this country yet. But in a world where every country is pervasively surveilling the citizens of every other country-- it's difficult to argue that we have a meaningful right to privacy.

That will require, I think, an international-- approach. And I'm hoping to learn from-- my fellow members of the panel about-- what approaches might-- might help in that regard. Been it's a conversation that has not happened yet in Congress and very much needs to-- if the government is to maintain the close relationships it needs with its intelligence allies and also to respect its international commitments-- to privacy.

And, finally-- Congress needs to set out for greater transparency to allow the public to be engaged, but also greater transparency so that the courts can be engaged. So that we can have meaningful review of these programs. There's a tension between the government's claims-- that these programs are so obviously lawful and so obviously constitutional, and the efforts to which it has gone to keep any court in public from adjudicating the lawfulness and legality of these programs.

If it's so sure, make the case to the court. Allow the courts to decide. And there are a number of proposals from members of Congress that would-- put us on the right path in some of these-- areas. There was-- a bill revealed last night from Senators Wyden and Udall-- Paul and Blumenthal that would go-- a significant way toward fixing many of the problems-- in this area.

So there are real solutions out there and there are people thinking very seriously, even in the intelligence committees. And we're hoping to support their efforts, both through our litigation and also through our advocacy. And, again, it's-- an honor to be here and I look forward to the conversation. (APPLAUSE)

PHILIP ALSTON:

Thanks-- Alex. I probably should have reminded everyone at the beginning about their cell phones. Please make sure they're on so the N.S.A. can get easier access (LAUGHTER) to them.

Next speaker is-- Frank Larue. Frank is-- was born in Guatemala. Is currently the-- U.N. special rappoteur on freedom of-- expression and opinion. I should-- I take it-- I should know that better. Frank and I were colleagues for a couple of years as special rapporteurs.

Frank is-- quite an extraordinary-- person. He has worked in the human rights field

in Guatemala for over a quarter of a century. He founded one of the major groups in Guatemala. He's been in exile for a long time. I first met him when I was in Guatemala in 2005 as special rapporteur on extra and judicial executions-- when Frank was in a presidential advisory position.

Even at that stage he was taking risks-- in a great many different directions. The fact that he is still with us is-- not-- was not entirely assured. He has been through a great many death threats. He has been extremely courageous in the Guatemalan context.

More importantly, though, for tonight's purposes, at least-- Frank has done an extraordinary job as special rapporteur. He's developed the-- a much deeper understanding of the significance of provisions that, at the international level, have for a very long time remained fairly vague and general. He's produced a whole series of reports which really have broken new ground.

He's about to present a new report to the U.N. General Assembly on the right to truth. But we're going to discuss tonight his last report, which was to the human rights council, which I understand was-- submitted two days before Edward Snowden presented (LAUGHTER) his report to the reset of us. But-- Frank's report is right on the topic of tonight's discussion. What can and should governments be doing-- in order to respect-- their international human rights obligations in the light of the sort of surveillance programs that-- Alex has described for us. Frank, welcome very warmly. (APPLAUSE)

FRANK LARUE:

Thank you Philip and thank you to the Human Rights Center of NYU for this invitation. And I also thank-- Sandy Coliver and the-- the-- our friends at the Justice Initiative of Open Society for this possibility of being here today. For us rapporteurs, there is nothing worse than to think that every report we do will be listened to, but then put in a drawer and lost in the walls of the palais de nacation in (UNINTEL) or in some building here in New York. It's much more interesting to be able to share these reports with students and civil society in general who will take 'em and research 'em and even take 'em forward and-- and-- and put into task.

I really must insist that I was not aware of Snowden when I did my report. (LAUGHTER) Some people say I had a leak, but no, that's not true. The-- the fact of the matter is that was-- an issue that was brought to me. Most of the issues I have taken were in response to the initiatives of civil society and the desire of civil society to highlight these issues.

And it was-- it was brought to me by efforts we had done with the Electronic Frontier Foundation and with Privacy International-- that-- they were very concerned about the fact that they were trying to systematize principles on privacy and other-- issues related to surveillance. We had been working with-- with the Justice Initiative on the shwani (PH) principles on-- on national security and-- and-- and-- possibilities of surveillance by the state.

And everyone was working on the issue, but nothing was being said officially within the U.N. And this is what prompted the idea of let's have a report. I must confess that I was stretching my mandate, because my mandate (CHUCKLE) is not on privacy. It's on freedom of expression.

But the logic is presented there, and I-- I strongly believed this, is that although freedom of expression and privacy are two very distinct rights, they must be understood hand-in-hand. Because if there is no privacy then you feel intimidated and there is a chilling effect to exercise your freedom of expression.

So freedom of expression can only exist, in reality, if people have the trust that what they say or they communicate or their right will be to the-- will be used for the destination they have desired and not be read by anyone else or used by anyone else.

This, by the way, is an issue related to national security and the role of the states, but we also raise in the report it's an issue related to private corporations because they facilitate the states. But also there's monitoring and surveillance being done for commercial interest, which is also a breach of privacy.

Because they're one thing to-- profile individuals and be able to send advertisements on this. Another NGO-- from South Africa, APC, a friend of ours, there was telling me that she put her photograph in one of the social networks. I don't know if it was Facebook or which, but she happens to be big, heavyset woman. And she says, "I'm very happy with myself. I've never had problems with the way I look or the-- how I am." But as soon as she put her photo she began getting a lot of advertisements of diet pills and the best (LAUGHTER) diet and the best exercise, all of which she had never requested.

So she says, "Clearly beyond the fact we-- we have the states monitoring us, we also have corporations-- the-- some of these social networks sending the information or the photographs to other people who are clearly trying to profile us and say, "Ah, this may be a convenient diet for this particular person."

Now what is the conclusion of the report. The report really draws attention to issues that, like Alex was saying, we're talkin' about civil liberties but also broadly we're talkin' about human rights. So there's nothing really dramatic. The dramatic is the reaction of the states, because they get-- they get scared.

One of the things we-- we say is that the communications of today are massive because of internet. And this scares those things. But the conditions that we should have for privacy should be the same ones we had before. The Human Rights Council. I did a report-- two reports, on-- on-- on internet freedom of expression in 2011. One for the council and one for the General Assembly in terms of access to that. And-- but in-- in the Human Rights Council they passed the resolution, which-- a phrase that we all supported and-- and that I have repeated, coming from them is very important.

Is all the rights we have offline we should enjoy online. Nothing really changes. Freedom of expression is the same if we're speaking, if we send a letter, if we make a telephone call or if we're sending an email. The difference is, of course, that if you

use internet it's much more massive. That you can-- I mean the difference that the internet brought is-- number one, is the speed at which it works, the amount of people you can reach, but the fact that it's an interactive nature of communication.

I'd mentioned that in my report. What scares-- scared many states and politicians was that before all means of communication had a communicator and had-- a destination. And specific sector of population. With the internet you could send out a message to a million people and they can respond in real time or they can communicate among themselves or they can forward the message to another million people each or they can network or many things can happen. And it is that potential that you're scared of.

So obviously this brought them to a panic and to the idea that this is the type of communication that they wanted to monitor. But the conditions of the rights of the citizens are the same. Many people were trying in the Internet Governance Forum, to establish a Bill of Rights of the internet. And I said, "No. We should maintain-- internet has challenges of its own from a technological point of view. And every new technology will have them." But in the same way that the digitalization process brought to telecommunications.

But the human rights principles of freedom of expression are there. And we have to apply the principles of freedom of expression that we have always had to these new technologies. And the same way happens with privacy. We should apply the principles of privacy and the right to privacy to these new forms of expression. Of technologies for-- for expression.

Now of course after 9/11 the debate change. And of course after Cairo and-- and-- and-- and Tunisia, the power of internet was seen. And even that accelerated the process. But here's where they brought us in to spiral of a false debate. It was-- we were talking with Aidan White.

Then for instance when 9/11 events happened, the press emphasized, rightfully so, that the logic here-- and this was seen by the press from Europe. But the logic here was let's look at the victims and their personal stories, and the effect, the dramatic effect, for the society. This is a legitimate story. I mean of course we must look at the victims always. And we must have a priority of the victims. And this is-- is reasonable.

But there was no other follow up of the state but just to look at the pain of the victims. And with the pain of the victims, and a pain that we all shared and suffered, came the justification that then we have to change our ways in terms of security. Beyond, even, what the Constitution allows or what the Constitution permits.

And here's where I say that the basic principle of national security, because in my report I don't deny that national security's absolutely a legitimate concern of every state. The state has an obligation to guarantee security. And-- and-- and I don't deny that there is more risks in the world today than before. The events in Boston recently proved that. Or the events in Kenya and Nairobi this weekend prove that terrorism is real and it can happen at any moment.

I'm not trying to say that that's not true, because that would be false. What I'm trying to say is that we must confront terrorism but within the boundaries of human rights. Marty Chinan, our-- our friend and past-- rappoteur, on combating terrorism-- within the framework of human rights, made that very clear in-- in-- in his reports.

And I try to apply the same principles to this by saying, "National security is to protect the individuals. But we not only protect the individuals. We must also protect democratic institutions. And in general we're protecting our democratic system."

So we cannot see protection of individuals separated from the other. We cannot say that we're protecting individuals and violating our democratic system, because that is a contradiction that inevitably will provoke a crisis. Because inevitably they will lead us to an authoritarian form of government. We won't feel it now, but we'll feel it down the road.

Because this will be the legitimacy of the abusive exercise of power, which is what all the constitutions were always designed to stop. Yes, the exercise of power is legitimate, but with checks and balances. And with participation and notice of society.

I always say, the most important element of the democracy, beyond the fact that you have a constitution, that you have institutions, the-- the most important element of any society is the participation of citizens. But this means the citizens must be informed.

But if think-- if issues are done or actions are taken, I-- behind the backs of the citizens, if citizens are not informed, if these are secret elements that are violating their civil liberties and their constitutional rights, then we're beginning to break our own democratic system. This is the danger.

So it's not really a foreign danger that we're talkin' about. It's a danger that we, ourselves, may begin creating cracks in our own system. And I-- I insist that the safest societies are the most democratic societies, because those are the ones that have the support of the population of their people.

And the most democratic societies are those that defend and uphold human rights and protect human rights. I always say that the protection of human rights is the-- actually the measure of democracy in-- in-- in any society. This is basically what the report has.

Then we present, of course, there have to be limitations to that privacy, like all limitations to freedom of expression, there can be limitations to that privacy. And how are those limitations in the communication? When there is a clear-- important human right to defend. You have in article 19, there has to be established by law. There has to be a very imperative issue-- in human right to protect. And it has to be necessary for the protection. And the measure you take has to be proportional.

So, yes, if you have a group trying to organize-- some terrorist activity, doesn't mean that then you should monitor everyone from a single religion or everyone from a

single nationality, because here is where we come in terms of the massiveness of the response, which breaks the-- even the principle of proportionality.

So what I say in the report is that all these measures should be taken with certain sort of checks and balances within the democratic system with the due process of law. Exactly like we used to do with the mail and the phone communications. There has to be a court order, as-- as Alex was saying.

I mean you need a judge to look at it and say, "Yes, there's a crime that was committed or could be committed," and to prevent, yes, a judge will order it. So there is a do-- a judicial oversight in this that will guarantee that this is not an abusive decision. And the best countries are those that have the judicial oversay in the parliamentary oversight.

The problem is-- here in the U.S. you have both, but the problem is when these oversights are beginning to be sort of modified-- in-- in the ca-- I had to correct my report because I had indicated-- in the examples I mentioned that Sweden did not have a judicial oversight. It turns out that Sweden just created a special court. So I did correct my report and I-- I apologized to Sweden. And I said, "Yes, now there is a court." But it happens to be similar to what Alex was saying. (LAUGHTER)

(OVERTALK)

FRANK LARUE:

It is a secret-- it is a secret court. It gives blanket authorization to the-- to-- they call it the numbers authority versus the intelligence authority. They-- they give blanket authorizations of monitoring. There is no other counterpart to the-- to the government that presents themself to this court. So no one really knows how these courts work. So it's not exactly your traditional and typical system of justice.

And why defend as a principle there? Is what we must never allow is that surveillance be decided by the government of any-- of any country, the central government of-- those that hold power, should never be decided by security agencies who may do it with the best of intentions.

But security agencies will always have their own particular mentality. And with little checks and balances. And even less by intelligence agencies. Because if we begin allowing them to make the decision by themselves, as we would say, per se, to make themselves the decision and monitor themselves the results, then who controls that power?

Who makes sure that that power eventually is not used for a political campaign? Because of course in the U.S. there's a tradition of an active justice system of a very important Supreme Court. But if we allow this, if the U.S. does it, which is what is happening in the debate in the U.N., many other countries begins saying, "Ah hah hah, well, then we can do it too." And maybe the justice system there is not as effective. Or the Supreme Court is not as independent. So the precedents that we

can create are very serious.

So here's where, again, repeating myself, we're not denying that there is a risk. Not only-- violence and terrorism, there's-- for Latin America, for instance, the risk is organized crime. Drug trafficking. And incitement to organized crime, including trafficking of people, trafficking of children, child pornography. All that is organized crime.

So there can be many, many forms of risk in that. But, again, all those risks have to be addressed within the legal procedures that the state has. And the state has to operate with its own checks and balances, with its own judiciary sort of-- monitoring and supervision. Parliamentary supervision. And be accountable to the people. That doesn't mean that you reveal all the information immediately. Now then-- and with this I'll finish.

MALE VOICE:

Yay.

FRANK LARUE:

We go into the pos-- possibilities of what happens with those that denounce-- what happens Snowden, to make it more specific? Because this news was my next report on the right to truth, which I would love to do it. Even here. We are talking that here at NYU.

But-- but basically if you know about a crime you have an obligation to denounce it. And if you're a public official that becomes a legal obligation to denounce it. Well, the same principle applies for me in terms of human rights. If you know about a human rights violation and you're a public official or related somehow to public-- and government activities, your obligation is to release that information somehow. To prevent that this violation continues. With no liability because you're actually defending human rights.

Now, this is a very sensitive question, but this is the fundamental issue, I think-- that we're talkin' about. Because of course it is not the say as someone is-- spying for a foreign power to threaten the national security of-- of-- of a country. That is a different matter.

But if what you're talking is of an individual who is not spying for anyone else, who is-- basically to his own public is denouncing human rights violations, then I think it is a very legitimate. Most crisis, legal crisis, in-- in-- in many country have been solved with leaks. From Watergate to the Pentagon Papers, et cetera.

So that should also be recognized today. But we're allowing ourselves in the debate of today, that we're trying to balance national security vis-à-vis the exercise of human rights and fundamental freedoms. And we should never let that debate go on

because there can be no balance. We need national security but we need with full enjoyment of human rights and fundamental freedoms. (APPLAUSE)

PHILIP ALSTON:

Okay. Okay, so-- (LAUGHTER) I think whereas I hope we're setting the-- ground work for a robust debate, because you can see the extent to which we have a somewhat one sided set of arguments (LAUGHTER) being point here. And I'm hoping that when it comes to question time-- there will be push back. If you guys think you're gonna get away with this.

So the third speaker-- is Katitza Rodriguez. Educated in Peru. Now the international rights director for the Electronic Frontier Foundation, one of the leading organizations working on all of these issues. Katitza has worked on a wide range of the sort of issues that we're looking at tonight and has been central in a lot of the international work-- around these issues.

And I think this will lead us-- at a certain point in the questions, of course, to what's the impact of the international work that you do, that Frank does, on the sort of stuff that Alex is trying to do domestically? Or are you in two different planets? (LAUGH) But anyway, Katitza. Welcome. (APPLAUSE)

* * *TRANSCRIBER'S NOTE: speaker's accent very difficult at times.* * *

KATITZA RODRIGUEZ:

Thank you. Okay. My first-- I work for the Electronic Frontier Foundation and I want to know if you can raise your hand if you don't know what the EFF is. (UNINTEL). Okay, good. But yet--

PHILIP ALSTON:

(UNINTEL) leave the room immediate, then. (LAUGHTER)

KATITZA RODRIGUEZ:

One minute. (LAUGH) The EFF is a not-for-profit organization founded in 1990 that was committed to fought for the (UNINTEL) rights on the internet. We see these early days that people were going to be using the internet constantly and that our rights was going to be challenge in a daily-- in-- in a daily basis.

And since then we have-- we are, like, a low view for the public (UNINTEL) and-- we have been defending internet use of rights since 1990 and taking one of-- some of the major legal challenges in the United States.

Internationally we do more policy and grassroots activism, working with-- with activists from around the world, from Africa to Europe and Latin America to-- I don't know. Canada.

Everything that it's outside the United States, that's my work. And I'm mainly focused myself on-- su-- surveillance. Fighting surveillance organizations and working with locals-- together to fight surveillance legislation in their own countries. And practices.

So as part of my world we have seen many litigations (?)-- the-- of increasing of the space veilance (PH) globally. We've seen, for instance, that some researchers in Canada (UNINTEL) a broad network of infiltrated computer systems-- that include a (UNINTEL) targeting for-- for the administrators, the media, NGOs and that the data that are wha-- being captured was sent to China. When Qaddafi surveillance regime was unveiled, we-- it was discover-- that difference in the United Kingdom foreign activists. Even (UNINTEL) callers-- where caught in different-- expansive web.

But it was-- it's not only other (UNINTEL) of regimes that are doing massive surveillance. Let's go to Europe. The European Union adopted in 2006 a very invasive mandatory data (UNINTEL) directive that compel ISPs and telecom services to collect the metadata, who communicate with whom for how long, for certain period of times, all (UNINTEL), all innocent individuals, for possible use for-- by law enforcement in the future.

And we have heard the-- the explanation of all the recent revelations-- that come (UNINTEL) and (UNINTEL). They selled you-- by your organization having fighting. So it's been eight years ago about the U.S.-N.S.A. surveillance program.

One of the issues that we care also, the international level, in the (UNINTEL), is the right of privacy of foreigners, because as was explain-- foreigner have (UNINTEL) rights in the United States, and not even the e-media take into account these.

And even my lawyers, the lawyer (UNINTEL) team, if I brought the topic, they said, "No," but I mean that have never been discussed. I-- I feel like a challenge. And-- but they are reacting why? Because of this everywhere. Because of the scope and reach of the program. And because most of the companies are basically U.S. and the in-- individuals-- are global. And so then are affecting and harming U.S. businesses.

So we-- one year ago we were seeing all these problems. Surveillance-- and the increasing use of surveillance technologies. So one year ago we get together with other leading NGOs like Privacy International, Access Now. Article N Team. But also traditional-- not only the-- digital rights in NGOs, but we tried to reach out to the traditional human rights NGOs and the media NGOs from around the world.

I would come up with a set of principles that try to explain how to apply exist human rights standards in the (UNINTEL) of surveillance. We took into account France report and we invite him to a meeting in Brazil where we have-- all these no-- and sharing of knowledge that inspire us-- to write the principles. So we come up with a set of 13 principles. You can find it on the web at Necessarily and Proportionate.org. And they are printed there too.

There are 13 principles that explain the problem of legality-- proportionality and the limitations to the right to privacy and how this should be applied in the digital context. The principles have been endorsed by 270-- organizations around the world.

And-- last week on Friday we have the opportunity to present it-- in front of-- many members of the Human Rights Council at the 24th session, on the twen-- Human Rights Council at the United Nation. The event was hosted by Germany, Norway, Austria, Hungary, (UNINTEL) states and Switzerland. And we have the opportunity to count-- it was an event where Frank was speaking. Nali Pilai-- the human rights commissioner from Human Rights was also-- I believe at the event.

The price-- the trece (PH) principles-- so provide this set of standards that we think can help to restore the rule of law-- in-- in this-- in this world. And what we came up with these principles? Well, when we were working on these we (UNINTEL) to find a lot of problems. And then we would highlight some of them-- to explain why we came to here.

So we were seeing a lot of companies issu-- issuing transparency reports, chain lighting (?) or how often governments demand access to this-- research data. And since then Google for the first one, I think it was a very-- first step. We have Microsoft now. We are giving these-- transparency reports.

But that was not enough. We see a lot of problems on transparency, on secrecy, that we were trying to fix with the principles. First, secrecy on gross industry transparency report. When some industries are now issuing transparency report, we see no transparency report in other industries. And telecom sector, (UNINTEL) sector.

So we have a total silence on transparency. We don't know how often governments are demanding data from-- our data from them. Then we see that it is fine that we from-- with transparency report we know how many times per a particular (UNINTEL) will be knocking the door of one of these internet companies and how many requests they were making. But we don't know-- me as as user, that actually my data wasn't (UNINTEL). And we don't know it was transferred to another country. Why? Because that's secret.

So we put the principles of user notification because in the traditional world, when we're-- there's search and seizure-- we-- the police go knock at the door-- show the warrant. And-- but we're, like, a notification in the offline world. But since we are in the online world, secret (UNINTEL)-- secret surveillance have become, like, the norm. We want to reverse that. So we have a principle of user notification. So-- and we want to place surveillance under the rule of law. And that's why the rule of law exists.

And we also see a lot of secrecy on transparency report from National Security Port Office. Of course, recently that whole Google are have been champion on trying to disclose even more information-- under ns-- N.S.A. request. And just a few days ago Lynn Carreen has also filed a motion with the FISA court arguing the right-- their First Amendment right to publish how many users are affected with FISA court.

But there are even more problems with secrecy of surveillance. Secrecy over government cooperation. We don't know the nature of their relationship between the N.S.A. and Google, Telecom, ISE or Microsoft, internet companies, which government are complicit with an-- (UNINTEL). Or which companies or governments are complicit with N.S.A. or the G.H.C.Q.

So government cooperation. The-- then we have secrecy over the nature of the technology. And recent leaks reveal that Balron (PH) program, a program that paint a picture of a spay-- a spy-- agencies working hard on the (UNINTEL) from in order to undermine their ability to communicate securely.

I leave a lot of-- key questions and answers. This means that N.S.A. has unfettered access to a huge amount-- huge amount of people's communications. To create a back door, government need a law-- to build a back door on the internet. You have the authority to give the power to the soul (?).

But the law does not exist. We were fighting a possible building in the United States. But this news reveal that companies are building weaker security (UNINTEL) that-- capabilities in their technology. In order to receive government re-- requests they're introducing insecurity in our tech approach. From a secret order, from a secret government department, we are creating a whole infrastructure of insecurity, revealed in our technology. That we-- that try to harm everyone.

And then we have secrecy over government power. According to *The Times* the-- U.K.-- the British equivalent to the N.S.A. had developed these new access opportunity in Google's systems. It means that the N.S.A. is actively building capabilities into the infrastructure.

The Times also speculates that U.S. government is hacking into com-- in-- in companies' computers, which is illegal basis. That's one of the principles, the principles of legality. We (UNINTEL) there and there (UNINTEL) law. The rule of law anymore.

But it's not only just seeing. That's how-- (CHUCKLE) something that is happening worldwide. We need to restore it. If-- like I say, these days, if we are just using the internet in a big-- big in-- daily day. And we're just disclosing all our data, not only what we put on the internet but what we do on the internet. And that internet that we love, that we defend, is coming a (UNINTEL PHRASE).

It's knowing everything what we know. So it's really problematic. And it become very problematic at the international level, because countries like China will say, "Well, if the U.S. can spy on foreigners openly, we can do the same." (LAUGH) You know? And that's the arguments that they use at U.N. (UNINTEL) sometimes.

So-- we need to s-- the U.S. (UNINTEL) see itself as the (UNINTEL) of the internet. But what the world now see is that the U.S. is not a stalwart (?) of the internet. This surveillance programs look like the actions of a country that simply exploding on wrong power over internet for very narrow missions. Counterterrorism with little public accountability. And even resistance to litigation under the states' secret privilege.

Or regard for its own (UNINTEL) and civil liberties. And-- we've seen repeat (?) that these level of global hell of internet, they think that you are putting insecurity over the infrastructure internet. How it will affect the global internet. How will afflec (PH) (UNINTEL). How it will-- affect the internet user worldwide.

We have seen (UNINTEL) for other estates, trying to buy, like, a nice internet. Compel companies to put a store service in their country to protect their privacy of their citizens. But we like our global internet. You know, it does-- what we defend, One War One, (LAUGH) planet one word. So we are in a difficult moment and I think that we need to start having a discussion in the United States about the privacy right of foreigners within the N.S.A. surveillance program. Thank you. (APPLAUSE)

PHILIP ALSTON:

Thanks so very much, Katitza. Okay. So the first thing is to announce that-- this session is being recorded. (LAUGHTER) But-- this time by us. No doubt also by others, but-- that's another separate question. So if you-- ask a question, just be aware that-- your question will be on record and the answer.

Let me start off-- I want to ask members of the audience-- and I'll take questions in clusters and then get the panel to respond. But just I think one-- s-- one-- reflection from a deeply pessimistic-- perspective on my part-- the human rights area is generally motivated or generally succeeds in its campaigning when there is strong civil society mobilization, and when there-- it seems to be in the interests of at least a significant group of governments to bring about change at the international level.

Do we have that in this case? Because it seems in the United States that this is sort of washing over. The new-- *New York Times* editorial page is deeply agitated by it. The ACLU (YAWNS) is also worried about it. (LAUGHTER) But it doesn't seem to be an issue that is really gripping the public imagination. And the same at the international level. Katitza brings us news that the Norwegians are agitated. The-- Brazilians, happily, because we-- spied on--

(MALE VOICE: UNINTEL)

PHILIP ALSTON:

--(UNINTEL) was-- agitated. But it seems unlikely that there's going to be-- a strong group of governments pushing to really take up your sort of recommendations from. So where's the mobilization goin' to come from?

FRANK LARUE:

It's-- it's a great question-- Philip. The-- there-- there's two-- there's two things that worry me. One is what you're saying. I think people are aware, but people see it as

something natural and necessary, because most of the information we're uploading ourselves. So people are assuming, "Well, yes. It's rather tragic that you're taking out that information," but the people uploaded most of the information that is on that.

Not necessarily the-- the-- the meta-- the metadata, the-- who communicated with whom. But in the social networks-- I mean people will give out even their address and their activities and their hobbies and to profile individuals are very simple.

So the-- I think the debate on what is more important, whether security or privacy, it's out there indirectly. And people tend to believe, "Well, as long as we keep safe and we can oppose any terrorist activity, we must sacrifice something." I-- I mean that's my feeling. This is why you won't have a constituency for a strong-- civil liberties movement or-- or constitutional rights movement on this topic.

PHILIP ALSTON:

Right.

FRANK LARUE:

And-- and-- and the other issue is the-- the question of technology because the-- the-- the corporations-- and Katitza was saying that as well. Corporations are coming to the conclusion-- because one thing is handing over information to the U.S., but another thing is handing over information in any country they work in, because if a country's a big market, for instance, and you want to sell your-- your services there, you will-- probably the government will put some restrictions in-- or ask you to hand over information to them.

And-- and-- and then you fall into the trap of saying, "In order to keep the market you will hand over that information." So one of the issues of the report was-- or even in selling the technology to rogue states or authoritarian states, so we were saying if there are, for instance, clear standards for selling weapons, and that there's sort of certification that they should not be sold to authoritarian-- regimes. Well, something similar should exist with the software for monitoring.

And then when you-- and-- and the-- the principles on access to information come in because when you try to apply for information or which states or which corporation are doing it, then they say, "It's national security. We can't give you that information."

PHILIP ALSTON:

Okay. Alex?

ALEX ABDO:

Can I present a more optimistic outlook? (LAUGHTER) Far be it from the ACLU lawyer to be optimistic, but I-- I actually think there is a constituency that's growing. And-- and I-- I think there is one in part because there is a consensus that runs across party lines that privacy matters.

And I wanna compare-- you know, I-- I-- had the misfortune of doing some work in the, you know, detainee realm where we're dealing with mistreatment. And I think that movement floundered in the United States in part because there was not a constituency domestically pushing day in, day out for accountability.

That the victims, at least in this country, were largely faceless-- and they were largely foreign, not marching on the streets to push for accountability day in and day out. Which I think contrasts that movement with what happened in Latin America in the '70s and '80s and up until today. There was a movement that lasted a generation.

And I think the privacy movement has the capability to be that type of movement. People are starting to recognize the invasiveness of this information. Companies are starting to compete over privacy. Microsoft and Google are going at it, for example, when it comes to whether they scan your email to serve you at. Microsoft's-- marketing ad right now is, "Don't Get Scroogled."

And I-- and I think that speaks (LAUGHTER) to a recognition, both that there is a business interest-- and-- a broader community of people who care about privacy. The NRA, after all, you know, filed a brief on behalf of the ACLU's lawsuit.

So did-- Representative Jim Sensenbrenner-- the author of the Patriot Act. A brief that was actually-- authored by the Electronic Frontier Foundation. So EFF and Jim Sensenbrenner joined forces to-- to help the ACLU. And that's-- something is going on when that happens. (LAUGHTER)

So I-- I think there is a constituency that's growing, but it's still in its nascent state. In part because people haven't always understood-- the significance of their online activities. It's generally been opaque-- but now we're-- we're seeing it.

And I don't-- I don't actually have a fear that the-- you know, the headlines today-- because they don't-- they're not all about privacy that they won't be tomorrow. There's a lot more information out there. There's more information coming and the story isn't dying. It'll-- it'll be back and it'll be back in force.

PHILIP ALSTON:

Okay. Great. Katitza?

ANSWER:

Well-- also positives. (LAUGH) I see a movement and I think-- surveillance is the--

the new copyright, we say in EFF. It's, like, the new battle. You know, when AFTA out-- everyone-- anyone familiar with AFTA? This-- a joint agreement-- that was sign-- by-- European countries and United States, so many others, that was going to put (UNINTEL) on-- propuluses-- with a sense of the internet.

Many NGOs, including us, have been working for years. We fought well (UNINTEL) that battle. And we will keep fighting and doing our campaigns. And suddenly, without knowing it, someone in Poland-- start protecting against AFTA. And it become huge protest and it's go wildly through Europe. And then we have this same experience with (UNINTEL) people in the United States--

(MALE VOICE: UNINTEL)

KATITZA RODRIGUEZ:

--in the United States. And it was a (UNINTEL) huge movement that come from this (UNINTEL PHRASE) way. And I see that surveillance is the next copyright in a sense of that there are some movement that is growing and our campaign-- that is a joint campaign with many organizations in the United States, Stop Watching Us, have a lot of signers. I'm-- up today with 1,100, more than half a million-- 500-- signatures.

In the U.S. with the principles-- we have been able to reach out to NGOs. Not only the traditional little (UNINTEL) but the human rights NGOs, (UNINTEL) NGOs, woman's NGOs and everyone is-- starts signing and getting involve in two (UNINTEL), even if they don't work on this issue. Just because they are caring.

So I feel like-- and I see on Twitter that people are still talking about the issue, so I think that it's a movement that is growing. And we have some countries that want to do something, like Germany or probably Braz-- Brazil. And probably there is opportunities to do it in a human rights council, for instance.

The U.N.s will be a (UNINTEL) at the-- for the ICCPR (?) vision in October. And that's a good opportunity. And civil society have ask-- Frank, I think recommend. Probably you can talk a little about the options in the United Nations that you're (UNINTEL PHRASE).

PHILIP ALSTON:

Well, hang on, let-- let's get--

KATITZA RODRIGUEZ:

You know. Okay.

PHILIP ALSTON:

--let's get to the questions on the-- on the table and then we can-- come back and see if that'll be relevant. Yes, gentlemen. Perhaps you should introduce yourself, if that's all right.

MALE VOICE:

My--

PHILIP ALSTON:

And-- and your--

MALE VOICE:

--question is--

PHILIP ALSTON:

--(UNINTEL) and present (UNINTEL). (LAUGHTER)

(OVERTALK)

MALE VOICE:

What-- what confidence do you have that there's really a legal solution to this? Because if you posit a national security state that's essentially lawless and, you know, you go into court and get-- court relief and they just disregard that, as they have just about everything else.

Why isn't the solution to this more technological? That you develop technology with state-- you know, can't eavesdrop. I just have a hard time-- the history is a complete string of lawlessness. And even brazen lawlessness or lying. I mean to the extent that Clapper gets in front of the committee and just lies about whether this is happening. And there's no consequence to that.

It just seems to me the track record is not particularly promising for kind of a legal solution. We tend to think that there are legal solutions to everything and it just-- it seems to me this is more maybe a technological solution is in order here. And I wonder if there are any technological solutions that are being considered or pursued, either by the EFF or ACLU or other-- organizations?

PHILIP ALSTON:

Okay. I would remind you that this is a law school and you shouldn't be casting aspersions on the ability of the law to govern. (LAUGHTER) (UNINTEL PHRASE). Let's take a few more questions and then we'll-- yeah. Let you do--

MARIA MCFARLAND:

Yes. Hi, Maria McFarland from Human Rights Watch. I now work on the U.S. but I used to cover Columbia-- work. And-- when I was covering Columbia I was-- working on a scandal involving the intelligence service, which engaged in extensive surveillance over human rights defenders, Supreme Court justices, critical journalists-- using equipment that the U.S. had set up for them, because they fed a lot of information to-- the D.E.A. and probably U.S. intelligence services.

I was wondering if you have any sense of how much-- information is going in the opposite direction. In other words, do you have a sense of whether N.S.A. information is going to other countries' intelligence services? And whether that might pose a threat as well?

PHILIP ALSTON:

Okay. Excellent. Yes, gentleman in the back?

TOBY MENDELSSOHN:

Toby Mendelssohn for (UNINTEL) Democracy based in Canada. I feel I should warn you that as a foreigner my statements are of important bearing on foreign policy and national security in the United States and you'll probably (UNINTEL) your telephone is being monitored for the next few months.

Now, I'd like to come back to the question that you-- raised. And I think that for-- a tough human rights campaign-- like this to succeed, it needs broad-based public support. And I think there I-- I-- I really agree with Frank. I think that we're-- we're losing the battle significantly in relation to private companies.

And-- I mean even though that kind of privacy may seem less important than national security monitoring, I think that psychologically it's having a bit of impact on us. We basically-- we're all on Facebook. We're-- 1.1 billion people have signed up for-- to Facebook.

And they have-- clicked on an oh-- an "accept" button-- and thereby given Facebook wide-- powers to use-- their-- their private data in ways that they don't know anything about because they haven't read the privacy policy. And in ways which-- the public are then-- you know, our kids especially are getting inured to.

And they-- and I have-- I have kids. And they basically feel that-- it's not that-- you know, that they're uploading the data and giving it to everybody for free. They're uploading it for their friends and whatever. But they are giving it to Facebook and they understand that that's gonna be used everywhere. And that change of values around privacy, which is happening, you know, visibly in the private sector-- is-- is-- is-- it's hard to-- to create the gap that-- vis-à-vis the public sector, when they basically feel privacy is lost to them.

And-- so I think that we need-- and things could have been different. This is a model which didn't have to develop in that way. Now-- that privacy-- sacrifice is built into the very economic model of these companies. I mean, you know, it's-- it's-- that's gonna be very hard to pull that back.

But it could have been different. And under European law those consent forms shouldn't really be accepted because they don't comply to the standards for data protection in Europe, but Europe's not maybe fuss about it because you can't really take on companies like Facebook and Google.

But I think that without bringing the public along with us and some-- somehow building back the sense that we do have a space that's private, vis-à-vis everyone, not just the government-- without that I think we're have a (UNINTEL PHRASE).

PHILIP ALSTON:

Okay. Great. Another-- yes.

DINAH PERCAPTIOR:

Hi. I'm Dinah Percaptior of Human Rights Watch. Several of you mentioned the need for there to be a debate on the international duvention (PH) of privacy in this country. I have a legal question for you. What would be your best argument that states, for example, states' parties to the ICCPR, are obligated not simply to protect the privacy of those under its jurisdiction and control, but those elsewhere. Those, you know, Frenchmen sitting in cafes in Paris.

(MALE VOICE: UNINTEL)

DINAH PERCAPTIOR:

I think that's an important thing, whether there is a legal argument or whether we're really only talking about public policy. And I'm-- I-- I know this is a topic to great debate, but I'm very interested in what you think the best arguments are.

PHILIP ALSTON:

All right. That's great. Let me take two more and then we'll-- get-- go back. Yes?

DAJI:

Hi. I'm Daji from Penn. I've worked with a number of the groups in the room-- so I've Access Now over there and CPJ. This is in response to your question-- about why people don't care more. It's something that we're interested now as well, we're working with the ASLU on this, which is how do you show harm in an open society if you're using a freemium business model like Facebook?

Most people are willing to give up a little bit but-- there have been surprisingly few social s-- social science studies done in this area. So it's actually a question-- we don't really know how we can show that we're being harmed by being watched.

But actually my question-- I do have a question-- which is about-- the metadata and encryption specifically. I find it-- I don't know how to describe this properly but-- if say 1% of people using the internet are-- child pornographers, or 0.1%, and you have an encryption technology like Tor-- which by its nature encrypts not just the content, but also some of the metadata-- metadata and-- and makes it possible for a criminal to hide.

In terms of the backdoor question, it's a really small percentage of-- of people who are using it for illegal purposes, but I mean-- I suppose I'm-- what would be the appropriate response? For a company like Tor or-- which is a non-profit, or for another company creating encryption technologies, should the government never be able to see-- what-- what the-- and-- the content is and how it's encrypted or whether the metadata's encrypted. And what-- how would you deal with that legally?

PHILIP ALSTON:

Okay. All right. Last question. Yeah, gentleman here.

FRED:

My name is Fred. I'm from Sarah Lawrence College. My question is about motive. It sort of relates to the last question. I-- I find it hard to believe-- and-- and I'm not a technical person, but out of the billions of people in the world and the billions and billions of data points that are collected, that it's actually possible for surveillance agencies, and the biggest computers they have, to get useful data out of all that. To actually-- to-- to be able to, you know, pinpoint suspicious activity when they're just drowning in so much data, apparently.

And it reminded me that someone, I don't remember who, testified that, you know,

originally that something, like, 50 plots were stopped by this and then later walked that position back I believe to just one plot (LAUGHTER) might have been stopped by all this.

So I guess I'm wondering if there may be something a little more sinister involved that might be about the chilling effect of just doing this, the sort of intimidating effect that it could have on the public of collecting all this data, even though it may not actually lead to very much useful results.

PHILIP ALSTON:

Okay. I mean I think those who work in the field of big data would-- tell you that in fact the-- it's-- there's much greater sophisticated capacity these days to make effective use of the vast and-- what we previously thought of as unmanageable quantities of data. But-- to let me ask the panelists-- don't try to answer all of the questions, each of you, but pick up on issues that you think have come out of them. We start with you, Katitza.

KATITZA RODRIGUEZ:

Okay. Regarding the question-- the intelligence agency-- I familiar with the case in the (UNINTEL) in Columbia. It's interesting case because the intelligence agency was dismantled for (UNINTEL PHRASE). The chief of the intelligence-- the agency's in jail. It remind me, yeah, (LAUGHTER) well, you know-- it remind me the case in Peru, 'cause I'm Peruvian, and we have the case of Fujimori which-- actually we-- he was doing illegal massive surveillance. Too.

MALE VOICE:

True.

KATITZA RODRIGUEZ:

He want to (UNINTEL) as well. But he's in jail and one of the crimes, because it was-- evidence that prove the intelligence agency was working for the president and he's in jail for several crimes. And one of them is illegal surveillance too. Now-- that's the case in Latin America.

But I know-- through leaks-- of-- Wikileaks published some leaks-- the diplomatic cables-- a few-- a few-- last year it was? A couple of years ago? And in those links-- there were some-- some-- emails-- where the united-- the government of Paraguay and Panama was-- talking on trying to use, you know, the-- DAE-- DEEF Corporation-- in Latin America for the (UNINTEL PHRASE) agency.

And they were-- in one to the mails the government was asking to visit for illegal purposes and the U.S. government was saying, "Oh, it's--" you know, they-- their private conversation was-- I have an article about that I publish in-- in *al Jazeera*. But it was saying, "Oh no, you know-- you know, we got away with this government."

"It-- there-- by be-- we might be violating-- international-- due process," et cetera, "because it's not-- it's for political purposes and it's not for-- for draft." But they also raise concerns that they're entrap (?) enforcement-- (UNINTEL) could be (UNINTEL) because they will not be able. Like, the government was threatening the U.S. government on cancel or close the surveillance program.

So-- and there is an interesting debate. I-- haven't published it and I just-- I don't even remember the details and I want to be precise on that. I don't-- have it over-- on top of my head. But I think that the (UNINTEL PHRASE) in Panama, Paraguay. And then I was researching along Mexico, because I think the reality Mexico's seen or to the reality in-- well, not-- not seen that, but it's complex as-- it was complex in Peru and it was complex in Columbia.

So that was part of one of my research. But I think the recent leaks reveal-- probably some cooperation with educate-- with the GAC-- Q-- about the-- the-- the-- I don't know some of the details, but about the cooperation with the U.S. with the Five I's-- Five I's (UNINTEL). And within the U.K. one. So that's what I know about, but I don't have more information beside what is reveal. Okay.

PHILIP ALSTON:

Okay. Thanks. Frank-- yeah.

KATITZA RODRIGUEZ:

Should I answer the others or not?

PHILIP ALSTON:

Not all of them, but if you--

KATITZA RODRIGUEZ:

Oh yes. Okay.

PHILIP ALSTON:

--yeah, just a quick comment on--

KATITZA RODRIGUEZ:

On the tech part, I remember there were two questions. EFF is working-- on *Surveillance Self Defense International*, which is a guide that guides-- activists on (UNINTEL) around the world how to take against surveillance. We-- we publish our newest edition after the links and-- pretty soon.

It will-- we also-- have a pa-- plug in that allows you to communicate anonymously. Well, not anonymously, but securely. And it's called HTTPS. You can find it. It's on our website. It's just put the browser by the (UNINTEL) HTTPS that allows you to-- to connect to URL with-- in a secure way. So yes, we don't see that legal is only the solution, but also we are realistic that-- no everyone use tag. I mean the regular user will not use PGP to encrypt their messages-- which is a secure program that I love, (UNINTEL) communicate-- securely.

And so we need all kind of actions. And I think that we need litigation and we need litigation probably at international level if pro-- is possible or regional level. And we need also-- education and encryption. And we need also activism. (UNINTEL) activism. Because it's a very difficult level.

PHILIP ALSTON:

Okay. Frank?

FRANK LARUE:

Maybe three-- three quick comments. One on-- on the encryption and-- the technological side. I put in my report-- all these-- encryption and anonymity are very controversial. And-- and not-- not so much in the U.S., but maybe countries around the world, especially Asian nations.

For instance, South Korea has something they call the Real Name Registration Act. To get-- to open an account you register with your real name. You put your address and all your-- otherwise you don't have-- an account, an internet account. And for them, anonymity is-- is a danger, a national security risk, that can be used for anything, they say. For criminal activity or just for bullying for (UNINTEL). They're not willing to accept that.

The-- also their standard-- tolerance for speech, or hate speech, and-- and-- not for hate speech but for offensive speech is much less because it has different implications in-- in oriental culture. So anonymity for them is-- unconceivable.

And for many other countries I find that encryption as well. They see that as a huge danger. Encryption is something that organized crime will not use.

But I put it in my report as necessary to defend-- privacy. I believe that anonymity is a way to defend human rights defenders. And, yes, it can be misused by the wrong

people. No doubt about it. But ultimately it's better to have it and well used than not to have it. The same way with encryption. Encryption can be misused but it's more important to have it.

But to tell you the truth I believe that both of them will eventually disappear. That I see the world in general moving into the mode of not allowing it legally and confronting it technically-- because-- because of security issues in-- in general. As much as I-- I defend them and-- no one has argued that-- against that in the report when I presented it in June at the Council. But you can see the mode and the-- the activity of that.

The second issue on-- on-- foreigners. This is something that will back-- I mean-- first, what-- what is the argument? I mean the argument is very simple. I-- I was invited by the State Department to present my report internally to them. And I did it. I-- and I enjoyed it very much and it was-- it was really, I must say, a wonderful conversation. It was very, very good.

And I had about 25 people from all different departments. From D.R.L., from human rights to the regional heads to the legal department to all the different section. And they were-- it was a very, very respectful, very high level conversation. I-- I-- I was very pleased.

But especially the-- the-- the people in the legal department kept on saying, "But you're wrong because we did amend the law," as you were saying. "We did amend the Patriots Act, because before we could monitor all incoming communication from abroad. Now, no. Now we do make a difference between who are nationals and who are foreigners, even if it's from abroad."

But I said, "I mean, look, if someone sends a message from Mexico and they're balled Paco Perres and sends a mex-- a message to-- to New York, how do you know if Mr. Paco Perres is an American citizen or a Mexican? I just-- there's no way. I mean it-- it--

(FEMALE VOICE: UNINTEL)

FRANK LARUE:

--to-- to find out. So it-- the principle is there, but-- but it really doesn't exist. And in contrast to that, I have a response. I said the most element is not whether a state can monitor-- foreigners or not. No state-- I mean in-- in human rights we-- we begin with the principle of universality. Everyone has equal rights, no matter what our origin, our nationality or our economic, social, racial, religious or-- or-- or any other form of origin. We all have the same rights.

And that cannot be violated by any state. So this is the position of the U.S. Yes. We defend the rights of our citizens. And the Bill of Rights applies only to American citizens, by the way, not to foreigners. But this is unacceptable in human rights, I understand. I mean human rights only exist for all human beings, not for any

citizens, not for any particular sector.

So I think-- and this argument will backfire on the U.S., because it can provoke a reaction the other way. When Velma Rosso saw her (UNINTEL), I'm sure that she knew they were one-- I mean-- I-- I'm sure there's no surprises in these things. But the fact that it was made public, for her it was a political problem in her own country. It was not a political problem with-- with Washington.

It was a political problem to the-- for her to the Brazilian people. If it comes out that she was being monitored she couldn't have-- an official visit. It would make her look weak. Turns out, it came out-- the-- that the-- the-- Washington knew before the Mexican public who were gonna be the future ministers of-- of (UNINTEL PHRASE). (LAUGHTER) How-- how do you explain something like that? And as-- as-- foreigners as they may be, but they-- they will say, "Look, my rights are the same as yours."

So I think it's a bad argument. A very bad argument. And I-- I've suggested constantly to my friends in the State Department, "Don't use it." I know that people feel that the Bill of Rights and the First Amendment are the high standard and that, yes. But don't use the difference-- the differency-- differentiation approach, because we-- we can't say that different nationalities, as we cannot say the different races. Anyway, the-- there's no differences. Universality should be the-- the-- the issue on-- on human rights.

PHILIP ALSTON:

Okay. Let's-- I wanna have-- another round of questions if we can, but--

ALEX ABDO:

Yeah, I just--

PHILIP ALSTON:

--Alex first .

ALEX ABDO:

I'll just be very brief. You know, it's-- there's-- it's a bit of an irony that the-- the same officials who are the ones who warn-- the American public and American lawmakers about the threat of cyber security are the same officials who are systematically undermining our best defense-- against cyber attack, which is technology, to some degree. Encryption data.

But, you know, systematically undermined-- the technologies that secure not just

communications between everyday people and also criminals, but communications between financial institutions. The type of technology that secures our medical records and other-- important information.

So I think there is a very important role for technology to play going forward. I don't think it-- I don't think we can rely upon it exclusively, 'cause today's technology will be broken by tomorrow's technology. And it turns out even if you can secure your communications in transit, it's very difficult to secure your computer itself. And it turns out it-- it might be very trivial for the N.S.A. to hack your particular computer.

But I-- I think that highlights what technology can accomplish, which is that it can make pervasive surveillance much more difficult. And if we can make pervasive surveillance much more difficult, dragnet surveillance, then the N.S.A. and other organizations, intelligence organizations, will be forced to use a targeted approach, which is the approach that they should be using.

And then we got a separate conversation about the extent-- to which they should be allowed to use certain tools in targeting their surveillance, but at least we're having the right conversation about targeted surveillance and not dragging surveillance. So there's a role for technology. I-- I don't think it's-- a quick fix, unfortunately, because it's, at least in its current state-- you know, secure communication technology and anonymizing technology, it's just not fit for mass public consumption.

And, you know, I think-- just to Toby's point, 'cause I think it's an important one. And-- and Daji touched upon it too. There is-- you know, there's obviously a relationship between the debate going on about privacy vis-à-vis corporations and privacy vis-à-vis governments. And I think-- you know, it-- we should-- explore those relationships, but I don't think we should lose sight of the fact that it's very different when a government gets access to information. That's nothing new. The government can put you in jail. Google can't.

But it does affect our expectation of privacy. It-- or it affects the way people talk about our expectation of privacy. And there's a circularity in U.S. law where the way we define privacy, at least if you look at some opinions-- opinions by some justices, is by asking what society is prepared to accept as reasonable.

And that in part is defined by what society has imposed as reasonable. You know? And there is a circularity there which I think is not helpful. I think it really is at the end of the normative question. What society should we want? And-- and as much as it is a descriptive question-- I think there's-- there's a role for both.

So-- you know, but as people become more aware of the threats of corporate-- aggregation of data, they become more concerned over governmental aggregation-- of data. And I think they have different solutions. But maybe people are willing to give up-- a little bit of privacy for a great email program-- but they're not willing for that same privacy to be shunted off to the government-- without any kind of, you know-- court-- correlative benefit to them. So--

PHILIP ALSTON:

Frank, one--

FRANK LARUE:

Can-- can I--

PHILIP ALSTON:

--one minute.

FRANK LARUE:

--just-- one quick-- very quick corollary to exactly what Alex was saying is that the question was this also-- with-- with the role of corporations is yes, you-- you're-- you're giving in your privacy to a corporation, but the other phenomenon that has happened means that corporations are being hired-- or-- I-- I-- we should take back that term. But are being-- are being forced by different governments-- I'm not talking about the U.S., to do the monitoring for them.

So what we're happening is that we're privatizing intelligence. This is a problem -- in all security matters. I mean a lot of the security activity is being privatized. And I have consistently said the state cannot delegate its functions. They-- to a private entity. Cannot hire private entities to do what is the responsibility of the state.

If the state wants to practice intelligence it has to do it within due process of law, for one. But, secondly, it has to do with itself. It cannot necessarily order someone else to do it, because then where is the standard? Who will monitor this private company-- to do it? No? Then--

PHILIP ALSTON:

Okay. Controversial set of issues. Yeah.

MALE VOICE:

Snowden at one point said he had authority to look at the content of-- of metadata. I never saw that clarified. I didn't think he had it. But if he thought he had it, he-- but-- but he probably exercised it. Is there clarity about whether he was-- anybody at Snowden's level was authorized? And whether the-- whether he did? Because if he did, it's even a worse problem below the big level if more people have this stuff.

PHILIP ALSTON:

Okay. Alex, you have a quick technical answer to that or--

FEMALE VOICE:

You know, I don't think--

PHILIP ALSTON:

--I mean (UNINTEL)--

FEMALE VOICE:

--we s-- have seen much clarity in the documents that have been released, but I think the point he was making is the broader one, which is that-- the-- protective measures in place are essentially executive protective measures. There's a self policing that's going on. You know, and we're trusting the N.S.A. to put in place measures that limit the access.

And it turns out that their public descriptions of that access may not be accurate. It might be they say only 20 people have access to the metadata database, when in fact -- anyone who is an administrator, like Snowden apparently was, could also have access. You know, it raises questions. I don't think we have any clarity exactly on-- on his comment, but there are certainly questions.

PHILIP ALSTON:

Right. And there's a lot more--

MALE VOICE:

I guess--

PHILIP ALSTON:

--revelations--

(MALE VOICE: UNINTEL)

PHILIP ALSTON:

--probably still to come. (LAUGHTER) Yes.

FABIA LATARION:

Hi. I'm Fabia Latarion from Access, Access Now. I'm curious to hear this question, both at the national level and the international level. Among the proposals that were brought in yesterday in Congress, it was-- one of them was Senator Blumenthal's-- creation-- bill that created a constitutional advocate.

I'm curious to hear your thoughts, whether that's actually an effective oversight mechanism. And it reminded me internationally a lot about the office of the ombudsman, the (UNINTEL) pueblo-- in Latin America. Whether they have work hand-in-hand perhaps with the judiciary in other countries to actually effectively protect-- due process.

PHILIP ALSTON:

Okay. Let's do some (UNINTEL). Yes, the lady over there.

CATHERINE FITZPATRICK:

Yes. Catherine Fitzpatrick. I wonder if the reason why there isn't more traction on this whole issue is that there are no cases. There's no real individual human faces, people that have been followed, that you can point to or people that were arrested illegally.

And-- to me that's really what's missing in this whole Snowden expedition, is that kind of human rights approach. If you have an anarchist approach-- and I-- and-- and it's-- and it's a lot about what machines' capacity might be. It's kind of edge casing about what might happen. Things that are dredged that might produce privacy. But there's no justiciable individual cases. And I-- I'm-- suspect there really aren't any. And-- and I think that's why we're not seeing it.

PHILIP ALSTON:

Okay. I mean I think that's an important element, the extent to which it remains an abstract threat-- as far as the-- great public is concerned. And until we can actually see-- see a face. Let's have a couple more. Gentleman in the back.

MALE VOICE:

I have a couple of points that were raised I wanted to address and one was the issue of limiting aggregate analysis. The-- you made the point how does one-- assume that the data is properly collected, which is a big assumption. How do you li-- limit aggregate analysis.

And the second one is-- Frank Larue's point about the privacy of destination. Is-- are there free expression problems in limiting destination to the motive of the-- of the sender? So freedom of information. The right to receive information. Is it-- how do you balance the right to receive information against privacy of destination?

PHILIP ALSTON:

Okay. A couple of others. Yeah.

MALE VOICE:

I think a couple of comments so far have eluded to a link between human rights and your, you know, state-based citizenship and the fact that human rights can only be guaranteed in the context. Or like (UNINTEL) guaranteed in the citizenship context.

And do any of you feel like when we go on the internet, in some ways we are surrendering those entitlements? That we have a more stateless identity when we go online that in some ways subjects us to a much weaker set of human rights protections.

And those things are implicit in our-- you know, our willingness to sign these agreements or to click on these agreements without reading them. But also just in the fact that when you're on the internet you don't-- you're-- you know, you're build to be a certain identity but you don't carry it with you the way that you do, you know, in a geographic space.

PHILIP ALSTON:

Okay. All right. Yes, gentleman here.

KEN HOROWITZ:

Yeah. I'm Ken Horowitz from the Open Society Justice Initiative. I-- I came in late, so I may have missed-- this, but-- how much do we--

PHILIP ALSTON:

I hope you've got a good excuse to getting here late. (LAUGHTER)

KEN HOROWITZ:

How mu-- how much do we know about what other countries that are not subject to any kind of s-- comparable public opinion or other controls such as China, Russia-- lots of other countries in Eastern Europe. I mean how-- are they-- is it-- it-- even if we were to s-- to be able to set up some kind of controls, a combination of technological and legal controls here-- what stops the technology from advancing in other places where they're not really subject to-- at least at this point, to-- to those kinds of political controls?

I remember that when Qaddafi was overthrown-- they-- there was newspaper reporting about-- people who'd broken into the Secret Service there. And it was mind-boggling, to me at least, that they had the capacity to listen to every telephone conversation into-- in-- in-- in Libya at the time. Of course it was European and Western technology that was allowing them to do that. But to what extent are we sort of-- a tempest in a teapot that-- that's actually much more sinister?

PHILIP ALSTON:

Okay. We've only got five minutes left. There's gonna be-- a brief reception afterwards, so we can-- but I think we have to-- give the panelists the opportunity to make some-- a final statement. Frank, do you wanna go first? I'm being arbitrary here, but trying to-- vary the order.

FRANK LARUE:

Two things. On-- on-- on the fact that human rights can only be exercised as a citizen-- that's a statement I-- I-- I would not agree on. Human rights are the responsibility of the state. This is true. But they are simultaneously the responsibility of all states and also the international community, which is why we have international standards.

So even if you are in-- in the sea, for instance-- out of the jurisdiction of any state in international waters, you're still exercising rights. You still have rights. Doesn't mean you have to be under the jurisdiction of a particular state or-- or be a citizen of any state.

It is true that most human rights are transferred into constitutional rights. And that certainly is the case in the U.S. when you talk about the Bill of Rights. But-- but that doesn't mean that that is the only way to enjoy human rights or that all human rights recognized internationally are registered in the constitution of every country either.

That should be the case but it isn't.

So I think we do have to make it very clear that we do have international standards that are applicable anywhere to anyone including in-- in-- in non-territorial areas of the world like international waters or international space or-- or whatever. As long as we're human beings. I mean-- and this is-- this is where the U.N. comes in. I mean this is why you have international bodies. So that-- that I think is an important-- distinction to make.

In terms of-- of-- of other states-- developing technology, I think the technology's being developed everywhere. The fact of the matter that some people have more capability-- some countries have more capability. Certainly the U.S. does and-- and even be-- before China I would say India has a lot of more research and-- and technological development. So we should have the pretention that although most of the advancement of internet is in the U.S. and Europe, that does not mean at all that research is not being done around the world.

And-- and yes, that-- that is something we have to-- something very contentious, which is why I insist that this debate on privacy is not a debate on the U.S. per se. I mean Snowden brought the scandal to the N.S.A. because of the massiveness of the information that he released. But the-- the-- the issue has to be raised with any state, anywhere. And-- and everywhere. Whether they have the technology or not, or-- or they're importing it from another country or-- or a private company is doing them the favor-- the fact of the matter is that privacy should-- should prevail.

PHILIP ALSTON:

Okay. Katitza.

(MALE VOICE: UNINTEL)

KATITZA RODRIGUEZ:

I did mention the Qaddafi example-- in my speech-- but I was talking about (UNINTEL) surveillance. Indeed that's a problem. We see not only in Libya, but we all-- with Qaddafi but we also see it-- with the-- these-- (UNINTEL) researchers that identify themselves in (UNINTEL), a lot of computers at work and documents that were stolen and sending it to an I.P. in China.

It-- or you also see in those proposals, like, in Germany that are using-- (UNINTEL)-- to spy on others. And when this is-- via email, but email could be-- not necessarily be in Germany. And so you still will do surveillance from the-- cross-border surveillance from-- from domestic soil. So the-- the U.S. of trojans or malwares on surveillance raises a lot of concerns to want these (UNINTEL) Russian (?) data debate.

So yeah-- we see-- we did also with another (UNINTEL PHRASE) because if you communicate with-- European then you're-- through email your ise-- I.S.P. of your

friend Euro will collect and store the-- metadata of (UNINTEL PHRASE) we home. And provided your data is captured the-- there too.

So I see a growing problem that is really-- very problematic. And you see-- a scenario that is very dark. But I think that we should not give up. That's why there is a need, as I-- mentioned in my (UNINTEL), to restore human rights in the court at the heart of the surveillance law.

And that's why we came up with these set of principles and tried to allied states around the world, at least to bring back the rule of law. And this is just one space. It's not solve all the surveillance prob-- problem, but at least to solve a piece of the puzzle that we consider quite important. And just to finalize, I want to give the URL of the principles. If there are more NGOs here we are open for signatures for NGOs, on-- experts. And-- so just go to the website-- website Necessary and Proportionate.org and you can read. It's in 13 (UNINTEL) now.

PHILIP ALSTON:

Okay. Good. Alex?

ALEX ABDO:

Sure. So just a couple comments. On your question, Claudia, about the constitutional advocate, I-- I, you know, have some reservations about bolstering a process that is too secret to begin with and giving it a legitimacy that I don't think it should have in our system of publicly adjudicating the meaning of our laws.

I think-- when courts decide what the contours of constitutional protections are, those decisions must be public. And I think those-- the-- the-- the litigation that surrounds the decision making should be public itself. People should be involved. It shouldn't be-- behind closed doors. And so I have reservations about-- you know, making that-- bolstering this process that is too secret to begin with.

And, you know, I wanna talk about-- briefly Catherine's question and then maybe she'll-- oh, there's Catherine. And the gentleman in the back. 'Cause I think the-- those questions are-- are actually relatively similar in my mind. Catherine's question was about-- whether there are human cases and whether that's the reason why the story hasn't picked up. And I think that's in large part true. You know, if you look at the abuses of the '70s, those surveillance abuses-- I think that really captured the public's imagination because there were specific and concrete examples of surveillance-- gone wrong. You had-- surveillance of Martin Luther King, Junior. You had surveillance of well known lefty and righty groups-- and-- and anarchist groups. And that surveillance I think really captured the public imagination.

I think one of the reasons why we haven't seen tho-- those examples could be in part because of the extraordinary secrecy that there still is, but it could also be because of the mode of surveillance that we're now entering. Whereas in the '70s the new

technology was being able to acquire those communications, now the new technology is being able to acquire those communications en masse. To get not just -- an extraordinarily detailed view of one person, but an extraordinarily detailed view of millions of people at a time. And that aggregated collection is the new mode of surveillance.

And I don't think whether we can put meaningful limits on that data once it's in government hands. The government typically argues that once it has lawfully collected information that you cannot lawfully restrict its use of that information. That is the general argument it makes. It doesn't always make that argument, but it frequently makes that argument.

And so I have concerns about trying to allow them access to aggregated information and then build in protections. I think the surveillance should be targeted at the outset to prevent the need to have to rely upon very difficult to patrol technical -- or legal limitations under use of that information.

PHILIP ALSTON:

Great. Let-- let's hope that the next-- Snowden revelations-- show widespread surveillance over Republican members of Congress and-- (LAUGHTER) specific leaders of the Tea Party. Then perhaps we'll get some action. Frank wanted one final--

FRANK LARUE:

Just--

PHILIP ALSTON:

--thirty seconds.

FRANK LARUE:

--two-- two very quick things that I-- I miss that I wanna mention. There is a danger in all this debate-- which is the fact that-- and it happened in this event where we were with (UNINTEL). In-- in Geneva the Human Rights Council on Friday.

That several states, I'm not gonna mention them, but that are trying to put the controls over internet were using the argument of, "Yes, since there has been the breach of privacy and since this is a problem, shouldn't we then have an international regulatory body control internet?"

And this is very dangerous, because obviously their-- their attempt is not to democratize internet. It's to re-- reduce and to control. And-- and more specifically,

even, if I work for the U.N. I can say that their intention is to move the internet governance to the ITU-- the International Telecommunications Union, because that is an institution they can move just by simple vote and who has (UNINTEL). Which doesn't make sense. I said an-- an internet is not a voting question. It's-- it's a multi-stakeholder dialogue.

But this is the attempt. So there is a danger that even in our good intention of bringing this debate abroad there's people on the opposite side that are gonna say, "Yes, you're right. There is a problem of privacy because-- there's too much surveillance. Let's have a regulatory body." So we must be very cautious and very careful of not falling into that trap.

PHILIP ALSTON:

Good. Thank you very much. I'd like to thank, again, the Open Society Justice Institute for having facilitated this and thank Frank and the other panelists for (UNINTEL PHRASE). (APPLAUSE)

* * *END OF TRANSCRIPT* * *