Global Encryption Day – October 21 2024 - Encrypt Today to Safeguard Tomorrow: The Encryption Summit

Encryption, the Guardian

Sharayah Lane - Internet Society: Thank you all for joining us for today's panel, The Guardian. And we are going to talk today about encryption and the impacts that encryption has on children's safety online. My name is Sharayah Lane. I am a Senior Program or excuse me, Senior Advisor at Internet Society. And also a member of our encryption team.

A lot of my work with the encryption team has focused on child safety online, and this is a relatively newer area that a lot of us are looking at. It will be a good discussion today. We have some wonderful speakers. When it comes to the topic of encryption and children's safety online, the discussion mainly has focused on perpetrators of abuses and exploitation of children online.

What we don't hear as much about, however, is the role that encryption plays in keeping children safe online. Today we will look at this topic with our panel of experts. Our panelists work in spaces that focus on children's safe use of the Internet. They are academics conducting research in the area, and the goal for today's session is for our attendees with a better understanding of how encryption plays a role in keeping children safe online, to support each of you, our attendees, in being better advocates for encryption with more information to add to your own areas of work.

And in addition to today's conversation, three of our panelists were also contributors to a collaborative working group document that delves deeper into this topic. If you're

interested in reading that paper, you can find it here, and I will just post that in the chat so you can find that paper here if you're interested in reading more.

But first I will introduce our panelists. First, we have Jessica Dickinson Goodman. Jessica bridges the worlds of technology and politics. She serves as a former board president for the Internet Society of the San Francisco Bay Area and supporting her team's exceptional work on tech policy, education, and helping underserved communities get better access to the Internet.She is also the author of the 2023 book, Encryption for Babies.

Next, we have Larry Magid. Larry is a Doctor of Education and is also CEO of ConnectSafely.org. He is a veteran technology journalist. He writes a weekly column for the San Jose Mercury News and is the host of the twice weekly ConnectSafely Report for CBS News Radio in the U. S. He is frequently a quest in national and local TV and radio programs, for the U. S. and the U. K. He served for 20 years as the on-air technology analyst for CBS News and is the host of the popular CBS show Eye on Tech.

Next we have Dr. Sabine Witting. Dr. Witting is an assistant professor for law and digital technologies at Leiden University. Her research focuses on the intersection of human rights, including children's rights, with digital technology. She is also the co-founder of TechLegality, a consulting firm specializing in human rights and digital technologies. Sabine is a non-resident fellow at the Center for Democracy and Technology.

Next, we have Dr. Ezequiel Passeron. Dr. Passeron is a Doctorate of Education and Society at the University of Barcelona with a graduate in Communication Sciences at the University of Buenos Aires. He also has a Master's in Teaching and Learning Environments Mediated by Digital Technologies. He is from the University of Barcelona.

He is the Director of Educommunication at Faro Digital, an NGO that studies and develops projects in media literacy. He is also Associate Professor at the University of Barcelona, Coordinator of Conectados al CERN Network. and Researcher in ESBRINA Research Group. His interests lie in the study and analysis of the intersections between education, communication, digital platforms, and artificial intelligence environments.

Lastly, we have Dr. Mark Leiser. Dr. Leiser is a regulatory theorist specializing in digital, legal, and platform regulation. His focus is on law and digital technologies. such as fundamental rights, e commerce, regulatory theory, platform regulation, contracting, security, privacy, freedom of speech, cybercrime, and phenomena related to deceptive design, dark patterns, consumer protection, and the use and regulation of AI and digital technologies.

So that is a lot of expertise on today's call. Thank you all so much for being with us and sharing your time and your expertise on the topic. We really appreciate it. So with that, we will go ahead and begin our conversation and we'll start with Larry Magid.

So Larry, you have worked significantly in the space of children's online engagement. Can you give us an overview on what you've learned about how encryption plays a role in young people's use of the Internet?

Larry Magid - ConnectSafely.org: Thank you. First, I want to acknowledge that there is definitely a large number of very well meaning people who have argued that encryption is necessary for law enforcement to prevent the exploitation of children, and they're specifically thinking of CSAM, child sexual abuse material.

There is controversy within the child protection community, and I frankly think that most of my friends and colleagues in this community would disagree with me. And argue that the need to prevent CSAM, which of course I agree with, but the, that's law enforcement's need, that encryption gets in their way and therefore causes harm.

And that probably does make the job of law enforcement more difficult. All issues have certain kind of nuances and trade offs, and by no means do I want to, in any way, diminish the importance of the blocking and prevention of child, of CSAM, so called child pornography, of child sexual abuse material, as well as the prosecution of those people who are trafficking in a way that harms and abuses children.

Having said that, it's also important to point out that children themselves need protection from the possible privacy and security violations that can occur with a world where there is no encryption. There are plenty of examples ranging from data breaches where children's data has gotten into the hands of criminals or potential criminals or where their information has been simply revealed in ways that violate their privacy.

There could even be an argument made. That encryption protects children against child predators because being able to get access to information of children about children makes it easier for those who want to abuse them to to find them and to reach them and to exploit them. And so this is a double edged sword.

But I, in, in thinking a great deal about it, I think that the, clearly, the ability to protect the privacy and the security of children is a fundamental right that must be maintained. And law enforcement needs to find other ways within the regime of an encrypted world to be able to enforce their desire their responsibility for combating child sex abuse material.

But there are many examples where Again, I mentioned data breaches, so I remember the National Health Service in the UK had a major breach a number of years ago with information about children. There are many cases of school data being breached and there are many cases of children themselves communicating directly with others in a way that could have been breached or maybe has been breached as a result of a lack of an encrypted platform.

So I do think that we all deserve protection. Whether it's banks and financial transactions, whether it's activists in a variety of countries, and by the way, children can be among the activists. When we think of people who are involved in activities that governments want to suppress, in many cases, these are minors that are engaged, teenagers, certainly, that are engaged in activities around the world, Where having the ability to have private confidential communications is essential not only for their mission in trying to reform things, but also for the protection of their own lives, because often there is a great danger associated with being part of a movement, regardless of how old you are.

And so there are so many examples that we need to point out. And I guess what I'm trying to do within the community that I operate is to get people to think beyond simply the law enforcement's desire. to protect, but the broader issue of protecting all of our security and privacy. And finally, and this was not an original thought of mine, but one of my colleagues that helped work on this document that you mentioned earlier made the point that encryption can often be used to help detect and prosecute crimes, but in, I'm sorry, the lack of encryption might make it easier to prosecute crimes, but encryption helps prevent crimes.

And given the choice between prosecuting and prevention, I would take prevention every time. It would be great to put prosecutors out of business because we eliminated crime. We'll probably never do that. But if we can reduce crime by protecting people's security, that means fewer cases of prosecutors have to go after.

Sharayah Lane - Internet Society: That's great. Thank you, Larry. And I wanted to move over to Jessica. I know that Jessica is going to have to jump off the call early so thank you for being with us. And my question for you is, what prompted you to write the book Encryption for Babies? What was your hope that readers would walk away with after, after finishing that book?

Jessica Dickinson Goodman - SF Bay ISOC: I've been interested in encryption since I interned at the Electronic Frontier Foundation when I was in high school, because I'm that kind of person and that kind of nerd. But at the time, I was staying at home with my kiddo, who will be two in three weeks. And I was reading him a lot of books about like astrophysics for babies.

There's a board book series that a lot of little kids have in the United States with statistics for babies and astrophysics for babies. And I wanted to explain encryption to him. I thought it'd be an interesting challenge and he's a smart guy. And he, and it's always complex, right? How do you explain something that's non physical, that's technical?

But I figured if we could read astrophysics for babies. We could figure out a way to talk about encryption. And so when I wrote it and tested it out on him, and then had my friends test it out on their kids, and then had a pop up event in downtown Mountain

View, and spent seven hours asking every technical person who walked by to try and challenge the metaphors I used there, and they found no technical errors, which was lovely.

And then putting it up online for sale to benefit my chapter back in San Francisco, my main goal was to help both the children and the parents who are reading to them feel more comfortable with encryption. Sometimes when you say I care about encryption, like I currently at Georgetown doing graduate work in the School of Foreign Service, and I wished everyone a happy Global Encryption Day for those who celebrate.

And not everybody will feel immediately comfortable with the idea. There is. Now a stigma attached to wanting to keep your children's privacy in some spaces, as Mr. Vedgett was talking about, particularly in the area that we both worked in Silicon Valley, where there is that very strong law enforcement narrative around trying to make their jobs easier around prosecution.

And I used to work for the California Department of Justice. I care about that work as well. But this is an essential tool for parents to be able to keep their family safe and understanding it well enough to explain it to a little kiddo is valuable rather than facing the tidal wave of scare tactics as trying to give parents a little rope to climb out from under all of that pressure to be anti encryption.

Because I think it's a good thing to do to want to protect your kid's location and privacy and pictures. And I can get into any technical details. with other adults, but my kiddo doesn't need to know about all those pieces. I will say, I was not sure if I was going to include the phrase E2EE in it, and it is my little one's very favorite part of the book.

He goes, E2EE! He thinks it is. Very fun to say that part and he asks me to say it over and over again. So sometimes we can get a little technical even with our youngest audiences and they'll be able to keep up with us, at least if they are fun to say out loud.

Sharayah Lane - Internet Society: I love that. I love that story. And I also am looking forward to checking out the book.

I have a little one that's right around the same age, so that'll be fun. Before you log off, Jessica, I wanted to ask you one more question while we still have you. You worked extensively on the role of encryption in protecting women's reproductive rights in the U. S. Can you share more about this work and how this connects to children's safety through encryption?

Jessica Dickinson Goodman - SF Bay ISOC: Absolutely. After the Dobbs decision was leaked, I went to my board for those who aren't familiar, most chapters are entirely volunteer based, so we started talking, we knew it was a sensitive topic but we wanted to empower people with information to keep their data safe. For all of the year that the

Dobbs decision was leaked, and as it came out, our chapter held monthly I call them tactical tech support trainings, open to anyone in the world.

I think we had a half dozen countries represented. A lot of folks from states like Texas that the government is actively seeking to gather private information. And we focused on two case studies. One was a young woman who was trying to seek abortion care. from Texas and needing to leave and needing to gather that information without, as has been the case, getting sued by a partner or arrested by law enforcement or having her friends or family sued or arrested or fined, which is currently the law on the books that's being challenged in Texas that a lot of people seeking abortion care are facing.

The other case study was of a young person who was in Alabama. And who was seeking gender confirming care outside of the state and had an in home concern. So those are the two case studies. So reproductive health care where you have a concern about the state snooping on your information and using it to throw you And the other was worrying about family members snooping and potentially being violent because of that information.

So we worked our way through what are the logistical issues, what are the technical tools. A lot of this was inspired by being, a queer person and a mom and a woman. And I need those tools. So that I can be free in the world in the same way that people without uteruses are free in the world, and the same way that straight people are free in the world, and I need to be able to have privacy because my government, though I aspire to work for it someday and have worked for it in the past, does not, it represents all Americans, not just Americans who agree with me, and who want me to be safe and happy.

And that series of trainings was important to me, and important to our chapter, and important to the people who came to them, because it walked people through how to set up WhatsApp, how to use Tor Browser, what is this? And most of the questions stemmed from that fear that Mr. Magic was talking about, that people were not sure if these tools were for them.

And if these tools were ones that were safe for them to use. And so once we talked about it, most folks were comfortable moving forward and using more encryption tools. But I think remembering that the people in government are just people and family members are just families and they are going to be good and bad and ugly and wonderful, just like any other person, and they don't deserve special access to location.

images or communication they can get a warrant just like they would have done a hundred years ago and get that information. They don't need to have special access just because it's 2024. So that's that was what we did and the training information is still online. The Electronic Frontiership Foundation has a wonderful digital self defense framework that we used.

Also the Plan C website, we use that for finding information about abortion care in it was important, and it's only getting more important as more states are passing laws to criminalize access to gender affirming care and reproductive health care.

Sharayah Lane - Internet Society: Thank you for that, and thank you for all the great work that you do.

I'm going to move over to Sabine. And thank you for being with us today. So you held a role with the UN working in Namibia and Zimbabwe on issues of law and policy reform on cybercrime private sector responsibility and digital technologies. What were some of the key findings that came up for you in this work regarding children's safety online and, or with the role of encryption?

Dr Sabine K Witting - Leiden University: Yeah, thank you so much. Thanks for having me. So yeah, as I was saying, I was working specifically with UNICEF for many years and in Southern Africa, but also in the East Asian Pacific region. And one thing that's emerging in a lot of global South countries is connectivity and access to digital technologies.

And of course that also means for children increased access and connectivity. And as much as. Digital technologies can be very helpful to, for children to realize their rights. Of course, there are also certain risks to, to children's rights. And particularly, I think the one that gets most attention is to the right to protection from all forms of violence, abuse, and exploitation.

And I think when we are, when we were working on these topics here in the region One of the things we always brought law and policy makers back to is to say, look, of course, it's an emerging topic that seems like something new, but the underlying dynamics of these forms of violence and abuse and exploitation are exactly the same that we have seen in the physical environment.

So when you think about how to prevent and respond to these kind of offences, you need to really think broader and not just think digital space, but really think about the entire child protection system and how you can make that protection systems stronger to also be able to respond to these technology facilities and cases.

So acknowledging this pathway between physical and technology facilitated violence was really very important to really come up with a holistic approach and not resolve to technical solutionism, which is something we still see very much now in not only the Global South, but very much so also in the Global North.

So I think that in the same vein, when we are Discussing these kind of policy interventions and specifically looking at the law enforcement side of things. So certainly

it's also a lack of appreciation for private communication and encryption. And I think it's also because we don't similarly value privacy and communication safety for children.

It just doesn't seem to be something on top of people's minds. Rightfully of course protection from violence is very much but at the same time, we really need to think across the entire spectrum of children's rights. And I think one of the things that was really quite quite telling for me was when we were working with children in Zimbabwe on the development of the Zimbabwe Child Online Protection Policy.

We asked children, so what's your experience online? What are the things you encounter? And there were, of course, a lot of kids that said we experienced various forms of violence, including sexual violence. But there were also kids that told us that they're using a VPN to keep to keep their And when we brought these findings back to the lawmakers in Harare, you could see a lot of the people in the room, the lawmakers, didn't know what a VPN was.

And I think this is quite quite an interesting aspect of the debate is that children's experiences and children's Children's focus on what is important to them in relation to digital technologies differs quite often from what adults think is really important. And we also saw that in the South Asia region where we were asking children what they want from tech companies to make digital products and services more child friendly.

And again, on the wish list, very high up on the wish list, was more data protection and privacy. And so I think this is For us and really for law and policy makers a good call to action in terms of consulting children, not only on the problem statement. So to what extent do you experience A, B, C, D, but also what do you think of the solutions that we're putting forward?

And I think this is where children's voices are very much lacking and actually not only children's voices, but the voices of all vulnerable groups that are affected by, let's encryption, as Jessica said. women, queer people, but also human rights defenders they would all their rights would all considerably banish.

And I think this is something where we are just not really taking the views of affected people into consideration that also includes children. Thank you.

Sharayah Lane - Internet Society: Thank you. And I do, we will continue that conversation a little bit later. With Larry, because I know that Connect Safely has a Youth Advisory Council that I would love to learn more about.

But first, I want to get to all of our panelists as we will then circle back and popcorn around to different questions for our different panelists. The next question is for Ezequiel. And this does actually continue off of Sabine's question a bit. Your organization works significantly with young people and their families.

What do parents usually do and do not realize that may be exposing their children? What can they be doing better? And what is encryption's role in all of this?

Ezequiel Passeron - University of Barcelona: Great. Thank you, first of all, for the opportunity to share with these wonderful people.

I think that we have to celebrate these spaces to have time and for dialogue.

I think that the first issue we see in, in families is the lack of intergenerational dialogue. In Argentina and South America, kids and youth are much alone in the digital world. Their adults are unaware of their practices and digital culture. So when a problem arises, They are not the people they, the young ones, turn to for dialogue.

In Faro, the main problems we are seeing when we talk and when we listen to students, to kids and youth are digital violence, mis and disinformation, an increasing personalization of the experience the filter bubbles, the lack of context with the difference, all the problems that these things are doing to, to social coexistence and democracy, and also the hyper sexualization and the monetization of youth imaginaries and subjectivities also. That's why in our NGO we promote to share moments of connection that encourage dialogue, conversations, trying not to judge about topics that interest young people in order to understand the care they need, I think that care, it's a great concept that we have to put in front. Beyond that, adult practices like I don't know, parenting, for example, emerge. That it's sharing personal images of kids and youth and that they see that it's a major problem and they don't like it.

Many children are starting to have a digital identity without even having consented to it. Regarding the role of encryption, we believe that it's a great ally for families because it's something that is generally unknown in our country. We studied the ISOC encryption guide you just shared and we see a great opportunity on delivering it at schools.

We think that this That kind of tools added to educational workshops and again, having time and space to dialogue and to build reflection could be an integral approach to reach these key allies in the protection and care of youth. Family often talks about parental controls or passwords or security screen time.

As Sabine said previously, the, we want a bottom to solve all our problems. And we think that encryption could be a really good technique to put it above the cares we have to have. From kids and youth.

Sharayah Lane - Internet Society: Yeah, thank you. It's so interesting this sort of shift in dynamic that's happened with even with things like regulation.

So it's always been the adult's responsibility to keep kids safe, in a number of areas. But when it comes to online and technology spaces, oftentimes younger people are more.

Informed, knowledgeable, and experienced than some of the older people. So it really shifts the conversation and the dynamic for how to go about doing that work.

Yeah, that is really important. I'm going to move to Mark for our next question. Another reminder, if you do have questions attendees in the audience, please place them in the Q& A feature. We have a couple that have already come in and we will be getting to those in just a few minutes so please do keep your questions for our panelists coming in and we will have time to answer them.

Academia plays an important role in research and research on how children engage online. What have been some of the key findings of your research over the years regarding encryption?

Dr Mark Leiser - Digital, Internet, and Platform Regulation: So I'm going to maybe cheat a little bit and start by, there was a great question that was in the Q& A, which actually I'm going to accidentally answer in part in my own answer to that question, so I just wanted to bring that to light.

So I would say that over the years, there's been countless incidents where encryption has provided children with safety in their digital interactions, but there's also been a gap in understanding its importance, which leaves them vulnerable. In the research that I've done, and obviously Dr. Witting as well, we found that unencrypted platforms expose children to risks. From location tracking, from metadata, to cyberbullying in unprotected messaging apps. In contrast, the use of encrypted systems dramatically reduces these threats. For instance, one case involving a child unknowingly sharing their location through a social media post, leading to strangers showing up at their home.

And so this incident, and others like it highlights how encryption can serve as a shield, safeguarding the sensitive data that we wouldn't want to fall into the wrong hands. But, children and parents still lack the education to recognize its value, which makes them susceptible to digital threats. And the micro narrative is to try and look at these specific incidents where encryption would have kept a child safe in a certain context.

But on a broader scale, the integration of encryption into platforms, schools, and gaming environments has had a substantial positive impact on child safety. So encryption prevents unauthorized access to personal data. It curbs identity theft. It reduces cyberbullying and stalking, and during the pandemic, the shift to online learning further underscores the importance of encryption.

When schools transitioned to encrypted video conferencing systems, it mitigated the risks, like the Zoom bomb and the digital intrusions into virtual classrooms. A gap persists in raising awareness about the role of encryption in protecting children online. As has been said before, the research and policy must converge to address these vulnerabilities by promoting encryption and expanding its implementation across platforms frequented by children.

And then finally, this sort of mega narrative. is that encryption is tied to the fundamental principles of privacy and security. And it has profound implications for digital rights and freedoms. While the EU's GDPR strongly encourages encryption as a method of safeguarding personal data, the global landscape shows stark differences in how encryption is actually treated.

In authoritarian regimes, restrictions on encryption enable mass surveillance, which undermines privacy and human rights. And the relationship between privacy and safety then becomes undeniable. They're not two separate things, they're two sides of the same coin. Encryption keeps people safe. It serves as a key pillar for protecting individuals, in particularly children and other vulnerable members of society, from the very exploitation and harm that parents are so desperately to do for their children.

As societies become more dependent on these kind of digital infrastructures, laws like the GDPR the laws that promote data protection and privacy by design are actually vital to ensure safety and the dignity of vulnerable populations across the world. Thank you.

Sharayah Lane - Internet Society: Wow, that was an excellent overview.

Thank you, Mark. And thanks for answering one of our questions. We've got some others coming in. So again, a reminder to our attendees, please feel free to type your questions to the panelists in the Q& A feature and we will have time to get to those a little later in our call. Our next question is for Larry, and this may inform some of what we've been talking about with including young people in the conversation and including them in the solution, ultimately.

So ConnectSafely has a Young Adult Advisory Council. How has working directly with young people influenced your work, and what are some of the key things you are hearing from them now?

Larry Magid - ConnectSafely.org: Having a young, a youth advisory board really grounds us in many ways, and it teaches us some of the things that young people strive to, and also teaches us some things that young people are concerned about. I have to tell you, in some areas, the young people are a little more conservative than I am when it comes to some issues.

It sometimes surprises me how worried they are about so many dangers on the Internet and how anxious they are to see some more controls put in. We have not had any extensive conversations about encryption. We do plan to do that going forward as part of our agenda, but I would imagine that we would have a difference of opinion.

That seems to be, one of the things you learn by talking to people in any demographic at all is that you cannot pigeonhole any demographic, whether it's gender, race, sexual orientation, age, or anything else. People are people with different opinions. But by and

large, I think certainly some of the young people that I've talked to have a very strong desire to see an Internet that is secure and private and really do understand the need for encryption in similar ways that Mark talked about and others as a way to protect them from potential abuses online.

There are others who might be concerned about the limitations or the challenges it provides to law enforcement, and that's something that, would be part of an education program to try to get people to get a better sense of the of why encryption is so important and how law enforcement could still do their job despite having tools just like they do their job despite the Various legal protections that have been in place in the United States and other non authoritarian countries, to the extent that the United States hopefully remains a non authoritarian country.

The but yeah, it's so important for those of us in the policy world to be talking to young people. And again, not making any presumptions as to what they might say, but giving them a seated table. As a matter of fact, this year, as some of Connect Safely is the U. S. host of Safer Internet Day.

And this year we're going to be having a policy conversation in Sacramento, the state government the state where the state capitol is in California, to try to provide young people with a role at the table so that when legislators are passing laws, Whether it's about encryption, or parental control, or age assurance, or social media, or so called anti addiction, or whatever else, that young people are part of that conversation.

We want to see an increased number. We'd like to see more education for young people about encryption. One of the reasons why Connect Safely has done a number of articles, and has been honored to be the host of the document that this group put together, is because we want to get, make sure that more and more young people understand encryption.

My sense is that most, to most people, it's an issue they just don't really have visited. So there's really a strong need to have a lot of conversation of education with people of all ages, but especially teenagers.

Sharayah Lane - Internet Society: Yeah, thank you. And I shared a link to Safer Internet Day in the chat if people were interested in learning more.

Larry Magid - ConnectSafely.org: Oh, By the way, we are giving out grants this year, as we have in the last couple of years, to educators and nonprofits. So if anybody wants to do a program on encryption in their community or in their schools, we have grants up to 1, 000 to teachers and nonprofit organizations to help them do community education around Safer Internet Day this coming February.

So please do check back in a couple of weeks when the applications are going to be launched.

Sharayah Lane - Internet Society: Yeah, thank you for that resource. That's a really great way to follow up from today's call as well. So I wanted to, with that actually move over to Ezequiel to continue this conversation because Ezequiel you also work really closely with children, young people and their families.

And I'm hoping that I can give you the big question and we can speak to the elephant in the room child sexual abuse materials, CSAM materials. I also seen a comment to this in the chat. So how do we protect from that? And what is in that toolbox? And what is some of the work that you all have been doing on that at FonoDigital?

Ezequiel Passeron - University of Barcelona (2): As I told you before, the hypersexualization of society, but also kids, it's a major subject that we need to face, and the way we interact with digital platforms has to do something in that scene. We don't believe in the determination of mass media on our practices, but it has a strong influence, no doubt about it.

In Argentina, we have significant work being done by specialized prosecutors in cybercrime. We know there's an extensive international cooperation, especially with the NMAC network. which facilitates the exchange of information on cases and the progress of investigation in each instance. The fact is that this kind of cases, we call it in Spanish, masi we have all the time this this misconception of kid pornography or infant pornography.

It's child sexual exploitation material and we have to. We have to say loud in order to understand the big problem. It is it's increasingly emerging. We have a lots of cases of kids and schools that doesn't know how to, what to do. So the, there's a key role there to engage with the prosecutors.

And police stations that are working this kind of cases. We also are seeing in our workshops that technologies like AI are being used to generate images of children that violate their rights and privacies. Last week we have a recent case that it was in the top of the news and media.

And how. Can we protect ourselves from this? And with what tools? I think that is the key questions to ask us. Once again, we emphasize in education, in digital citizenship and creating spaces of dialogues. I think that this kind of sexual things are sometimes a little bit taboo in our societies.

But when kids are on the Internet and in between digital platforms, there's no taboo. We learn by doing. And most of our times before having a space to question, we to discover our sexuality with with our parents with a confidence adult. We believe that

education, we believe that dialogue and create space, safe space for kids to, to express their curiosities and all the things they need to learn step by step are the main thing we have to promote and to defend.

Sharayah Lane - Internet Society: Yeah, and there really is, so many different ways to look at this. There's no one clear answer and I think that is really at the heart of our call today is the addressing the issue That when it comes to encryption and the impact on children's safety online, so much of the focus has been on perpetrators of abuse and has been on adults and the community.

implications of encryption for young people online gets really lost into that conversation. So how to go about maintaining a safeguard for young people online through encryption while prosecuting and addressing the issue of child sexual abuse materials Is an open question right now, and it's something that a lot of people are working on and thinking through.

And and it really is the one of the great challenges of the moment because as we've heard from our speakers before the number of ways that encryption plays a role for young people. So to just take it away has an effect too. So thank you for a little bit more context on that. I know that one's always a difficult question.

And Sabine, I wanted to move back over to you. You have done work extensively advising policymakers around the world on technology. What is one of the key things that you advise policymakers on when it comes to children's safety online?

Dr Sabine K Witting - Leiden University: Yeah, and thanks so much for that question. Of course, we always come from a human rights and a child rights background.

What our kind of key advice is really that we cannot isolate children's safety and their right to protection from other children's rights. And as under the UN Convention on the Rights of the Child, all these different children's rights, they are interdependent and they are indivisible and interrelated.

So this means we cannot advance one right without considering the adverse impact or the positive impacts of other rights in the convention. And what that looks like in terms of advice, what law policymakers should do concretely when they are in a situation where they think about laws and policies.

The first step for child online safety is to really conduct a human rights impact assessment, including a specific focus on children's rights. And what that means is to really use the methodology that's been put forward by the UN Guiding Principles on Business and Human Rights, actually, to think about, okay, which are the affected human rights across the board, not only for adults, but specifically for vulnerable population and children.

And then a second step to think about, okay, to, to what extent. What extent are these rights impact? So what's the scale? What's the scope across various jurisdictions? And I think this is one of the things we always highlight that even if you are the EU and you are considering policies that impact end-to-end encryption, you must know that this has an impact on laws and policies across the world.

And As you said, we work on these on these policy decisions across the world, and I can't tell you how many times we have seen provisions, for example, from the UK Online Safety Act, copy pasted into new cybersecurity laws where the context obviously is very different in countries where the rule of law might not be equally respected, and that is of course a huge concern.

So once this human rights impact assessment has been done, we need to really think about, okay, so what measure can we now put in place that considers all these different affected rights? And this is where the term proportionality becomes important, and I think when we look at the debates around child unknown safety and end-to-end encryption.

Everyone claims that their measures are proportionate. And what strikes me is that people seem to think that proportionality doesn't really have a methodology to it. It's just something that you feel if one or the other is more important, then you just. claim proportionality of that specific measure.

And I think, of course, coming from, I'm from Germany, and I work a lot in the EU, and we put a lot of emphasis on the methodology behind the proportionality tests. And there are two things I would like to highlight. First one, is to ask, is that measure really necessary? Do we have any equally effective but less intrusive measures?

And only once we have exhausted these measures, then we can think about more intrusive measures. And I think when we are thinking about less intrusive measures, like these systematic approaches to strengthen the child protection system, I think we're still failing considerably across the board. If you look at some The assessment of child protection systems also in global North countries.

The narrative is almost always the same. We don't have enough social workers. We don't have enough law enforcement specializing in these issues. Teachers are not trained. Doctors are not trained to identify cases of abuse and exploitation. So my question is, even if we were to detect all of these images of image child sexual abuse, then who's going to respond to that?

And. So the answer is probably no one, because we still don't have a sufficiently equipped child protection system. And I think this is where, we really need to think about whether this measure is really the best way to go about this problem. And the second point is about the proportion, proportionality test per se where one of the first

steps is to really assess, okay, what, to what level is a specific right And that level of infringement has a red line, and this is what we call the essence of the right.

And once we have reached that essence of a specific right, then that's a red line. And then it doesn't really matter, what's on the other side of the scale, so to speak, then this right is infringed. cannot be infringed. And this red line, I think, is something we really need to think about when we talk about abolishing or weakening end-to-end encryption in the context of private communications, because I would argue that red line has probably been reached.

This is something I think that is not really discussed sufficiently, and where we really need to go back to the basics of human rights law, really, and really assess from a holistic perspective what this measure means to human rights and children's rights across the board. Thank you.

Sharayah Lane - Internet Society: No, thank you.

And thank you for bringing up the convention to having a way to measure. Something to measure against is really helpful and I've read the sort of convention on children's rights and I think there are so many things in there that are relevant and that align directly with encryption and children having access to encryption online.

But again, it is an ongoing conversation so I wanted to move over to Mark. You have done a significant amount of research on the legal side of technology. Are there currently any laws supporting encryption that we should know about? If so, what might be their impact? If not, why do you think that is?

Dr Mark Leiser - Digital, Internet, and Platform Regulation: There's very few laws that actually say you must have, I don't think there's any laws that are like the Encryption Act or anything like that, but we do have a number of laws that, in effect, support encryption. As a European academic working alongside Dr. Witting and in the Netherlands and in the UK.

The GDPR obviously has a there's the fundamental sort of data privacy, data protection law for the EU with extra territorial effect and some might even argue the Brussels effect in that other countries have to adopt. in order to comply with our rules and to have access to our market.

There's two or three different things within that. First is, Article 25 obligation data protection by design and default. So if it is if you're building a technology where you could protect data protection, or you have to protect data, then by integrating encryption at the inception stage it's not a mandatory obligation to do it, but it helps get companies thinking about the risks and taking steps to ensure that data is safe and secure.

Now, why is this important? Because, under Article 32, Data controllers and processors are required to implement appropriate technical organizational measures to secure personal data. And one of the things that is highlighted to ensure data security is encryption. Now, what's the impact of that? The impact of that is that under the GDPR, if encrypted data is compromised in a breach, But remains inaccessible due to strong encryption, the penalties for the company might be significantly reduced.

So it becomes a major incentive for companies to actually implement encryption protocols. The fact, the second thing is, as I hinted earlier, is that The GDPR has a ripple effect on privacy and data protection laws around the world. Many companies, even those outside of the EU, adopt encryption as a best practice for compliance.

Global tech giants like Apple and WhatsApp and Google have leaned into end-to-end encryption in part to align with GDPR standards. And WhatsApp's end-to-end encryption ensures that only the communicating parties in theory can read the messages. Even preventing the company itself from accessing the content.

Now in the U. S., the CCPA, the California Consumer Privacy Act, which is often seen as the U. S. equivalent of the GDPR, emphasizes the importance of securing personal data. So it's not mandated, but it's treated as a mitigating factor when assessing penalties for data breaches like the GDPR. If a company experiences the breach but can prove that the compromised data was encrypted The liability and the damages can, could be reduced and the CCPA has actually become a catalyst for federal and state privacy laws.

If you build laws in the model of the CCPA incorporating encryption becomes a recommended security measure. The kind of unknown quiet law on privacy and data protection in the EU is the E Privacy Directive. And this is often referred to as the cookie law. And this governs the confidentiality of communications within the EU.

The idea here is that the, this law and the proposed regulation that will replace it, It's expected to strengthen the role of encryption to ensure the confidentiality of electronic communications. These laws in themselves, you can go to Brazil, you can see encryption as a standard security practice for companies operating in Brazil.

It helps encryption shows that they've complied with the LGPD and also to main competitive in the global markets. And then you have other sector specifics, like HIPAA in the U. S., the Health Insurance Portability and Accountability Act. Again, it doesn't mandate encryption, but it does provide healthcare providers health plans and their business associates to implement technical safeguards to protect health information.

And so it's an addressable safeguard, meaning that while it's not mandatory, while it's not mandatory, It must either be implemented or document why an alternative measure is sufficient. So even the susceptors like HIPAA the expansion of encryption into health tech, As we are building entire systems for the sharing of health data from one provider to another, to work with doctors and hospitals and insurance companies

and whatnot to sharelessly and seamlessly port health data over one place to another, encryption is seen as being the tool to protect those protect the privacy of that communications.

There's some in Australia's telecommunication and other legislation amendment under the Assistance and Access Act. There's another example of looking to mandate encryption. The one final point is why aren't there more laws mandating encryption? So in some areas, it comes down to balancing national security and privacy.

We touched on that in my previous discussion. Governments are hesitant to mandate it because it could interfere with law enforcement and national security operations. In other developing countries, it appears that the legal infrastructure to support encryption hasn't fully evolved, and so you don't have privacy laws on the books, and so encryption hasn't always been prioritized.

And the third is actual pressure from authoritarian regimes. So encryption is viewed as a tool that can enable dissent. Thereby weakening state control over information. As a result, some regimes are actively discouraging the use of encryption or are imposing legal restrictions on it. So you can see the sort of dichotomy between privacy and security and authoritarian versus democracy.

And I think I know what side I want to be on and I'll leave it at that. very much.

Sharayah Lane - Internet Society: Yeah, thank you for that overview. And I think that we will likely continue some of that conversation in our next panel as that will be an important topic. And what's so interesting about the legal side of encryption is that you do see such a difference where, some places are, Working to legally protect this right to privacy and some countries are working to totally dismantle.

And it's just interesting that there's that there is such a big difference between the 2 and to see these different trends around the world. That's a major part of our advocacy work at ISOC is looking at encryption laws or laws that would undermine encryption around the world and doing advocacy work on a global scale.

So that was a great overview. Thank you for that. I think we have time for one more. I'm going to go ahead and ask our individual question before we get to our Q& A. Last chance, we will be moving into the Q& A portion, so if you did have questions for our panelists, please place them in the Q& A feature on Zoom, which is going to be down by the chat button and the participants button on your screen.

Last question, I wanted to come back to Ezequiel. And I wanted to ask, what is something important, and I'll just say something because I'm sure there's many things, but what is something important that you have learned in starting an organization like

Faro Digital about young people's experiences online and how we can work toward better experiences for them in the future?

Ezequiel Passeron - University of Barcelona (2): Great. Thank you for the final question. In the recent years, due to the attention economy, the way platforms operate, we have noticed a growing interest and a strong influence on the subjectivity of young people regarding what we call as monetization. This refers to the pursuit of gratification and rewards in every action, a common future of any social network.

That creates a dynamic where the Internet or the digital space is perceived as a source of income from home without seemingly little effort. Practices such as online gambling where Adults, we are very concerned, but when we go to workshops and listen to youth, they don't see it as a shameful conception.

So there's a very big gap or breach we need to fulfill. The sale of intimate images, the investments have emerged in Argentina. A regulation has been in place for a few weeks, allowing individuals over 13 years old to enter the financial market. And that regulation, it's not something isolated. Thank you.

It, it refers to a practice they have in their online in their online practices. So what we see as a problem or more as a challenge is that the issue of trust. Which leads them to, to fall victim to digital scams, for example. In Argentina, we talk about Poncidemic a problem that is fueled by the emergence of these young influencers they call them Poncipros.

They're all the time like, bro, you have to invest in this, you have to take this course, they are supposed influencers who encourage other young people to become their own bosses, having free time, make a lot of money every month from their sofas. Of course they are the old Ponzi scams that existed previously Internet, but that now they found out in digital platforms as vehicles to recruit and to attract more people, especially in economical e economically disadvantage context.

In the digital world, we live in as a territory where our attention is exploited where our emotions and desires are at the center of the business of big tech companies That's why we need to create, that's why I talk about creating time and spaces just in brackets, we like to figure it out as a metaphor.

We need to protect, we need to care we need to create these spaces where kids and youth can develop together with others. Where they can study and practice world affairs without a goal, an objective, or utility. Just trying to understand the world and renew it, as Hannah Arendt told us half a century ago.

Our time is the time of this big problem, Wilson. CODIS, we have Paleolithic Emotions, we have Maya Deedle Institutions, and God Like Technologies. We love that phrase. We

think we are in a time where we need to recover the sense of the phrase of Descartes, of Cogito Ergo Sum. When we think about that phrase we translate it as, I think, therefore I am.

But when we study the etymology of the word cogito you can find out that it both refers to I think and also to I care. So I leave you a question. Who are the ones in our society that are in charge of care practice? I think that there's a huge and rebel revolutionary issue that we have to fight and defend to put cares In another place in our society.

Thank you.

Sharayah Lane - Internet Society: No, that's such an excellent reminder that so much of the challenge or the problem or the issue is the way that we're looking at it. And the way that we're approaching things I think that so much of how we've approached these issues thus far have been from. And a sort of outdated perspective and understanding and the need to really think deeply about these questions and to really understand what young people are facing and what they're going through and to take the time to understand that.

All of these things are so important in our larger conversation. Thank you for bringing up the sort of philosophical side of this, because I think it is a missing piece. Missing piece of the conversation. So we are going to, we have just a few minutes left. We're going to get into our Q& A from the audience.

I have a translated question here. It says, I, and this is for any of the panelists, so feel free to jump in and answer. I found the encryption of children's images interesting. As a protective factor against the use of images from this user or non user profile, depending on the child's age, could encryption be used to search, select, and remove images of children who do not have autonomy in expressing their will?

Larry Magid - ConnectSafely.org: It could certainly be used to hide those images to make sure they're not shared by, without the consent of a child or their, who, I'm not sure it could be independently used to search for them. Maybe some of the more technical experts have an answer to that.

But it certainly can protect the privacy of those images just to make sure they only get to the people who they mean to share them with.

Sharayah Lane - Internet Society: Yeah, so as a sort of retroactive piece, or going back and removing and hiding images, I don't believe that encryption can be used as that sort of tool, but it's more of a preventative feature, so it would prevent Thanks. Thanks. The unauthorized use of images to begin with, but if it,

Larry Magid - ConnectSafely.org: if there is a, at least in the United States, if there's a sexually explicit image of a child that's online, you can go to, I believe it's takeitdown.

org, it's a service of NECMEC, and have it removed, and then there are a number of sites that help fight revenge porn and other Distribution of intimate images of adults as well. So there are tools you can use to take them down, but I don't believe, as you said, that you can retroactively encrypt them.

Sharayah Lane - Internet Society: Okay, and I'm just getting the link to that resource. I will put that in the chat as well. And with that, I know that I believe that Mark answered this a bit in his response, but I will also pose it to the whole group. When it comes to legislation and policy regarding child online safety. There is a trend of top down proposals, rather than measures that could empower parents to make informed decisions about their children's online activities.

For instance, one flavor of proposal is to legally restrict minors from using social media after certain hours. Is there a balance between necessary government imposed rules, such as data privacy laws in the U. S., and empowering parents. And it says, feel free to challenge my framing entirely.

Dr Mark Leiser - Digital, Internet, and Platform Regulation: Can I add to my answer?

Sharayah Lane - Internet Society: Yeah.

Dr Mark Leiser - Digital, Internet, and Platform Regulation: Sabina had her hand up as well. I'm sure she's got something to say to this. I think it's important for parents to realize that children have a right to privacy from their parents as well. And that we often talk about this as being, something that we want to give parents to have more control over.

But I also think we need to recognize that the new norm should be that children have a safe space to communicate free from the parents. And I'll give you a couple of examples just very quickly to hammer this point home. The first is, there are very, there's many cultures where being LGBT is frowned upon inside the home.

And if you're going to be exploring your sexuality, your sexual identity, you want to be able to speak freely, independent of your parents snooping and looking into your communications. The second and the more obvious one for people in Western cultures, I think, especially in this day and age, is people who are looking for information on sexual health and their identity.

And then the third is to actually protect the child from communications that might be harmful or unwarranted or unsolicited. So if you give them a safe space for them to communicate, then the child is actually empowered to keep children out. So that's my

addition to the question, but I think it's also important to recognize that parents need to have, provide child a safe space where they can communicate freely independent of oversight by the parent.

And I'm sure Sabina will have other thoughts on that as well.

Dr Sabine K Witting - Leiden University: Yeah, thank you, Sabine. Yeah, thanks so much. I think Mark also touched on that point. I think when we always then focus on parents instead, we say oh, we shouldn't do or we should not infringe on anti encryption. We should focus on digital literacy and the role of parents.

And I agree with that. And I think to a certain extent, there is a misconception that we think that parents always act in the child's best interest. And I think that's certainly not the case. And Mark mentioned a few examples from I think that's where that actually might not be the case, so putting the parent in charge will necessarily make the child safer, and I think that's something to consider.

And I also think in this debate, there is a bit of a, it's a, There is either a focus on end-to-end encryption or digital literacy, and it's either we use this or we use the other measure. And I think that kind of lets tech companies off the hook a bit too quickly. Because even though we don't want them to create loopholes or back this end-to-end encryption, we want tech companies to do to create a safe environment.

For children and that should be done through legislative efforts, and Mark and I have written a book chapter on it, which I think will come out next year, where we look at the Digital Services Act, for example and the kind of measures that the Digital Services puts in place on intermediaries to actively create a safe environment for children such as mandatory reporting of illegal material, creating child friendly reporting mechanisms, and noticing.

And so on and so forth. So I think there is certainly a big role for digital literacy, but we should not only put the responsibility on parents or children and just let the tech companies off the hook. Thank you.

Sharayah Lane - Internet Society: Yep, I agree. Thank you. And Larry.

Larry Magid - ConnectSafely.org: Yeah, it varies by country, but in the United States, there is a, I wouldn't say a consensus, but the culture is built around the idea that parents control their children and have all the rights of a child really flow through the parent, whereas Europeans have a somewhat different attitude, I think, there and the fact is as Mark so properly said, it's, Children need a certain degree of autonomy, even from their own parents, and not only for the reasons that Mark specified, and they were all very good ones, that a parent might actually have a different attitude towards reproductive health, towards gender identity, towards sexual orientation, etc.

But also, not all parents are comfortable or equipped to engage with authorities, and even social media companies might be seen as an authority. They may have concerns about immigration, that somehow, by getting active in, in, in doing something online for their children, they're going to raise the possibility of them getting into trouble with the immigration authorities.

They may not have the literacy, either the technical literacy or the language literacy. They may not be aware, and there are children who, unfortunately, have parents who are otherwise ill equipped, maybe because of mental health issues, or simply the fact that they, their lives are too chaotic or too busy, etc.

Not all children are served by their parents and not all parents are equipped to provide the kind of support and permission structure that some of these laws require of them. So I do worry about children being left behind for all sorts of reasons before, and so before any of these laws are passed.

We need to think about the unintended consequences.

Sharayah Lane - Internet Society: Yeah so important. I want to thank you all for joining us today. We have about 6 minutes left together and, I would like to ask as we close, I would like to ask each of our panelists 1 closing thought, so a sentence or 2 regarding encryption's role in children's safety.

So the question for you. is why is encryption important to you when it comes to children's safety online? And we can start with Mark.

Dr Mark Leiser - Digital, Internet, and Platform Regulation: Myself there. I think in a sentence or two sentences, at the societal level, privacy and safety are not just linked but mutually reinforcing pillars. Thank you. functioning, a functioning democracy. So when children feel empowered and secure, knowing that their personal information isn't going to cause them harm, this contributes to a broader sense of child safety and trust in both the digital and the physical environment.

And by weakening privacy protections can then lead to a loss of safety. And I think that when you prioritize. Privacy and safety for the child. You ensure the protection of their rights, their civil liberties, and their trust in digital technologies.

Sharayah Lane - Internet Society: Wow, that's good. Ezequiel, we'll move to you.

Ezequiel Passeron - University of Barcelona: It's complicated to go after Mark.

Thank you for that. Yeah, I think on one side that we really need to make broader questions in order as Sabine told us before we try to we always try to think at a

technique solution for the problems we have in our relationship with techniques. I think that human nature is technique, right?

Without having a shared language, we can't understand ourselves here. That's why we think that we need to start to find out new ways and paths and techniques in order to safeguard our primary rights. I think that empowerment of kids and youth is vital. I really think that this metaphor that it was created in 2001 of Digital Natives, I think it was, it came out as a major problem For us adults to take care of children because we think they know everything of the digital world and that we can't help them.

I really think that the encryption is a safe way in order to be empower in, in, in a territory that is in, on this boot where we have a lot of a lot of companies trying to, to. To make business about our time and attention and I really think that this time of techniques can save our rights and be and just having powerful environments for us to live there and to enjoy and not being exploited, I think that's in a few words.

Sharayah Lane - Internet Society: Yeah, no, that's great. Thank you. Sabine?

Dr Sabine K Witting - Leiden University: Yeah, I think I think if we continue to polarize the discussion as it is at the moment, I think we are creating a perfect distraction for the two stakeholders that actually should invest in prevention and response, which are the governments by really investing in the child protection system, but also the tech companies, and really creating safe and rights respecting products.

So I think this would maybe be my appeal is to really take a step back and ask Cui Bono and that's certainly governments and tech companies. Thank you.

Sharayah Lane - Internet Society: That's so important. Thank you. And lastly, Larry.

Larry Magid - ConnectSafely.org: I think that all people, regardless of age, are entitled to privacy and security and entitled to have communications that are just between them and others.

And I think, after listening to the speakers and thinking about our role, we need to flip the script. On this notion of child protection and not allow people who think that child protection is simply by empowering law enforcement to giving them all of the tools and surveillance tools that they need, but also protecting people from criminals, from family members, if necessary, and acquaintances, from governments that might oppress them.

Or just because they want to have private communications. And then finally, I think we need to double down on education. It really makes me think, as I contemplate Safer Internet Day and the work that ConnectSafely is doing with teens, that we all need to

provide teens, and children for that matter, With every tool that we can possibly give them to help them protect their privacy and their security.

And that's in addition to all the things that we continue to do around phishing and passwords and also, we teach them how to use robust encryption as a way of protecting themselves.

Sharayah Lane - Internet Society: Yeah again, thank you all so much. We had a wealth of expertise and knowledge on today's call, so I really appreciate you guys for taking the time to share with all of us today.

We have some great resources in the chat, so please feel free to follow up on any of the links that were shared today, and attendees, for joining us today, and we hope that you can join our next session, which will be starting in about 10 minutes. called Encryption Arrested, the arrest of Telegram's Pavel Durov for failure to register encrypted services.

So again, that sounds like it'll be a little bit of a follow up to our legal conversation about encryption and law today. So if you would like to take a break, you'll have about 10 minutes before our next session for Global Encryption Day, but thank you to our speakers and thank you to all of our attendees for joining us today.

All right. Thank you. Bye.