TRANSCRIPT
Event
“Launch of the United States Guidance for Online Platforms on Protecting Human Rights Defenders Online”

DATE
Friday, March 29, 2024 at 9:30 a.m. ET

FEATURING
Kelly Razzouk
National Security Council Special Assistant to the President and Senior Director for Democracy and Human Rights

Ambassador Robert S. Gilchrist
Senior Bureau Official, Bureau of Democracy, Human Rights, and Labor, U.S. Department of State

Wai Phyo Myint
Asia Pacific Policy Analyst, Access Now

Alexandria Walden
National Security Council Special Assistant to the President and Senior Director for Democracy and Human Rights

Jason Pielemeier
Executive Director, Global Network Initiative

Sheryl Mendez
Senior Program Manager, Emergency Assistance Program, Freedom House

CSIS EXPERTS
Michelle Strucke
Director, Humanitarian Agenda and Human Rights Initiative, CSIS

Transcript By
Superior Transcriptions LLC
www.superiortranscriptions.com
Good morning, everyone. Welcome to the Center for Strategic and International Studies. I’m so delighted to have you here with us today, and delighted to have those who are all tuning in online for this very important discussion of the launch of the United States Guidance for Online Platforms on Protecting Human Rights Defenders Online. I want to thank our partners in this effort, the United States Department of State as well as Access Now and the Atlantic Council’s Digital Forensic Lab, for all their support in putting this event together today.

My name is Michelle Strucke. I’m the director of the Human Rights Initiative and the Humanitarian Agenda here at CSIS. And today, as – in 2024, according to the Digital 2024 Global Overview Report, 5 billion active social media profiles exist in the world. As a percentage of global population that is 62 percent of the world that is engaging in social media. Mobile phone users now are up to almost 70 percent of the global population, and more than 66 percent of all people on Earth now use the internet. So this issue is affecting the daily fabric of all of our lives as they change and become increasingly reliant on social media platforms for our commerce, our entertainment, our utilities even and how we pay our bills, all the way to how we engage in networks.

And people who are experiencing some of the positives of this are human rights defenders, but also some of the negatives, of people who are the dark underside of the – of the internet, that’s being used to track, threatened, target, and harm people, including human rights defenders – the very people that are upholding the values we all care about, of human rights, democracy, and other important issues. And human rights defenders include everyone from members of NGOs, and trade unions, to environmental advocates, and land rights activists, women’s rights champions, and anticorruption activists and representatives of indigenous people. So really, some of the most important people that we rely on to fight for human rights are being impacted positively and negatively by this issue.

So, it couldn’t be more important than it is today to have this discussion. And I’m really glad you decided to join us. For those who are watching in the room, we have the recommendations listed on here on the screen, and you can also use your phone to scan the QR code if you want to look at the full report. For those following online, you can also access that to see. I’ll give a couple announcements. Just that if there’s any emergency, the emergency exits are right behind you and the bathrooms are down the hall. Again, it’s my pleasure to be with you here today. And I will now introduce the special guests that we have here, that are going to share with us some important thoughts.
So, first, we will have remarks by Kelly Razzouk, who is the National Security Council special assistant to the president and senior director for democracy and human rights. Kelly currently serves at the White House National Security Council as special assistant to the president and senior director for democracy and human rights. And prior to this she was acting chief of staff and deputy chief of staff for policy for the U.S. ambassador to the United Nations, Linda Thomas-Greenfield. From 2018 to 2020, she was the director of humanitarian policy and advocacy for the International Rescue Committee, IRC, where she represented the organization at the United Nations.

And she's held numerous U.S. government roles throughout her career advancing key U.S. priorities at the U.N. in New York. She’s also served as a human rights ambassador to Ambassador Susan Rice and then as senior policy adviser to Ambassador Samantha Power where she led key human rights initiatives for the Obama administration, including efforts to secure the release of political prisoners around the world. She’s had a distinguished career as well as a civil servant, working in a variety of important State Department bureaus. And she has a juris doctor from DePaul University College of Law, where she was a Sullivan human rights law fellow. So I couldn’t be more delighted to introduce Kelly here to the podium to kick us off with some keynote remarks. Thank you. (Applause.)

Kelly Razzouk: Thank you so much, Michelle, for that introduction. And thanks to all of you for being here today. It's such an honor to be at the Center for Strategic and International Studies. It's my first time here. And I'm so thrilled to be in the room with experts from civil society, from technology companies, from governments, and to host this launch in partnership with Access Now and the Atlantic Council's Digital Forensic Research Lab.

Technology, as Michelle said, and as all of you know, has fundamentally transformed the fight for human rights around the world. Online platforms enable activists to mobilize and share information more quickly and more widely than ever before. But at the same time, human rights defenders across the globe too often face technology-facilitated threats and attacks, such as targeted surveillance, censorship, and harassment. These attacks can also move from the digital to the physical world. The misuse of commercial spyware, for example, has been linked to arbitrary detentions, disappearances, extrajudicial killings, and transnational repression.

A woman was physically attacked and sexually assaulted for her advocacy highlighting the growing hate against LGBTQI+ people online. A reporter, focused on exposing acts of corruption, was murdered at a carwash after being targeted by commercial spyware. And these are just two of the stories. Last week, at the third Summit for Democracy in Seoul, the United
States convened a high-level side event focused on the misuse of commercial spyware. And the reason we highlighted this at the Summit for Democracy is because it’s both a national security and counterintelligence threat, but it’s also a very real threat to democracy.

My colleague, Maher Bitar, who serves as coordinator for intelligence and defense policy at the White House, and I co-moderated a panel at the summit that brought together ministers from countries, journalists, civil society, and private sector experts – like representatives from the investor community – to discuss the importance of exposing the misuse of commercial spyware and protecting human rights defenders. The journalists talked about the fear they had, not only for themselves but for their loved ones who faced profound risks to their safety and security. Their comments reflected what I’ve heard over and over again as I’ve had the honor of meeting with heroic journalists and human rights defenders from around the world who have been victims of online attacks.

They’ve described the chilling effect that commercial spyware intrusions have had on their ability to continue their reporting and their activism, the isolation they faced from colleagues and counterparts who now feared any contact with them. One prominent Russian journalist has publicly described an intrusion by commercial spyware as, “feeling like she was stripped naked in the street.” Online attacks are all-too-often gendered as well. Around the world, an estimated 85 percent of women and girls have experienced or witnessed some form of online harassment and abuse. Indeed, gendered information manipulation and nonconsensual synthetic content are frequently designed to silence and suppress women political and public figures, by forcing women to self-censor or limit their online activity.

The growing access to and use of artificial intelligence further exacerbates these harms, by expanding the speed and scale of intimidation, manipulation, and synthetic content – including nonconsensual intimate images, facilitating highly targeted and pervasive surveillance, and enabling enhanced and refined online censorship. The companies and civil society organizations represented here know these harms all too well. Many of you have reported on the insidious tactics of nefarious actors that use online platforms to target members of civil society, journalists, and activists. Addressing these threats is critical not just for the individual survivors of attacks, but it is also a global imperative for the defense of inclusive representative democracies.

The United States government remains resolute in our commitment to address these harms. As President Biden said at the second Summit for Democracy, we must ensure that technologies are used to advance democratic governance, not to undermine it. The United States helped
develop this guidance that we are launching here today for online platforms to support governments, civil society, and the private sector to come together to fight back against these human rights abuses. This platform guidance is part of a whole-of-government effort to – as Secretary Blinken explained last week at the third summit – to build an inclusive rights-respecting technological future that sustains democratic values and democratic institutions.

Last March, the president issued an executive order prohibiting U.S. government use of commercial spyware that poses risks to national security or has been misused by foreign actors to enable human rights abuses around the world. Over the past year, the United States has leveraged sanctions, export controls, foreign assistance programs, and visa restrictions to support victims and hold governments and firms accountable. We’ve built a global coalition of countries committed to this cause. In fact, last week at the summit in addition to hosting the site event that I just mentioned, we also announced that six new countries would join the joint statement on efforts to counter the proliferation and misuse of commercial spyware, adding to the inaugural 11 countries.

Additionally, the Cybersecurity and Infrastructure Security Agency at the Department of Homeland Security has been partnering with many of the organizations and companies in this room to protect high-risk communities, including civil society organizations and human rights defenders, through their Joint Cyber Defense Collaborative. And at the first Summit for Democracy in 2021, the Biden administration launched the Global Partnership for Action on Gender-Based Online Harassment and Abuse, which brings together governments international organizations, civil society, and the private sector to accelerate progress towards safety and accountability for women and girls online.

One thing we know to be true is that we cannot do any of this alone. We need the expertise of civil society actors, the private sector, and online platforms. Today’s launch is a starting point for these important conversations that will take place going forward as we look to continue to strengthen these partnerships. Thank you for your time today, and we look forward to the conversations and the work ahead to address these critical issues. (Applause.)

Ms. Strucke: Thank you so much.

It is now my pleasure to introduce Ambassador Robert Gilchrist. He’s the senior bureau official in the Bureau of Democracy, Human Rights, and Labor at the U.S. Department of State. Previously, he served as principal deputy assistant secretary since September 11th, 2023. He’s a career member of the senior foreign service, class of minister-counselor. His last
position was United States ambassador to the Republic of Lithuania, from 2020 to 2023.

Prior to being ambassador, Mr. Gilchrist served as director of the Department of State’s Operations Center, deputy chief of mission to the U.S. Embassy in Sweden, deputy chief of mission to the U.S. Embassy in Estonia, and the director of Nordic and Baltic affairs at the State Department’s Bureau of European and Eurasian Affairs. And among his earlier assignments in his distinguished career, he was also the deputy political counselor at the U.S. Embassy in Iraq, chief of the political section of the U.S. Embassy in Romania, and a special assistant in the Office of the Deputy Secretary of State. So please join me in welcoming Ambassador Robert Gilchrist. (Applause.)

Ambassador Robert S. Gilchrist:

Thank you, Kelly. Thank you, really, to all of you for joining us this morning as we officially launch the U.S. Guidance for Online Platforms on Protecting Human Rights Defenders Online. I’d like to extend my thanks to CSIS, Atlantic Council, and Access Now for cohosting this event, and to many of you in this room for your insights, inputs, and reflections during consultations we held over the last year as we developed this guidance.

I’m Robert Gilchrist, a senior bureau official in the Bureau of Democracy, Human Rights, and Labor at the Department of State. Human Rights defenders, or HRDs as we call them, play an integral role in promoting and protecting human rights. And governments and private sector companies should take steps to protect HRDs, and respect for the rights and values for which they so fearlessly and tirelessly advocate.

The United States developed the Guidance for Online Platforms we’re launching today in response to the rapid growth of online threats against HRDs around the world. We remain resolute and our commitment to put human rights at the center of our foreign policy, and to condemn attempts to silence human rights defender’s voices through threats, harassment, criminalization, or acts of violence.

We are grateful that the EU shares this commitment and is working with us, through the U.S.-EU Trade and Technology Council, to elevate the voices of defenders and underscore their essential role as individuals on the frontlines, defending human rights. On March 11th, we released a joint U.S.-EU recommendations outlining 10 steps companies can take to better identify, mitigate, and provide access to remedy for digital attacks targeting HRDs.

U.S. guidance builds off those recommendations by providing specific actions and best practices companies can take to protect HRDs who may be targeted on or through platforms, products, or services. This guidance
is addressed broadly to online platforms that host third-party content, but we also hope it can support collaboration within the broader ecosystem, including with civil society organizations who directly work with human rights defenders and act as trusted partner organizations to these platforms.

I also want to clarify who this guidance is designed to protect. The United States defines human rights defenders as individuals working alone or in groups who nonviolently advocate for the promotion and protection of universally recognized human rights and fundamental freedoms. Defenders can be of any gender identity, age, ethnicity, sexual orientation, religious belief or nonbelief, disability status, or profession. Some HRDs identify more readily as journalists, labor leaders, environmental activists, community leaders, researchers, lawyers, or volunteer election observers.

HRDs continue to face threats and attacks, including arbitrary or unlawful online surveillance, censorship, harassment, smear campaigns, disinformation – to include gendered disinformation – targeted internet shutdowns, and doxing. And online attacks often pave the way for physical attacks, including beatings, killings, enforced disappearances, and arbitrary detention. As threats to defenders and democratic values escalate and evolve, preserving safe spaces for HRDs to work online is more important than ever.

As Kelly mentioned, the U.S. government takes a broad approach to protecting democratic values online. At the State Department and within DRL, my bureau, we are committed to supporting and protecting HRDs so that they can carry out their essential work without hindrance or undue restriction, and free from fear of retribution against them or their families. In Washington and throughout the world, department staff maintain regular contact with human rights defenders.

Our embassies have dedicated human rights officers who regularly monitor human rights developments, meet with defenders and their families, and advocate for our shared principles. Over the past decade, the department has provided $60 million to directly support almost 10,000 human rights defenders from more than 130 countries and territories. From journalists to anticorruption actors, and environmental defenders, to labor activists, this often lifesaving assistance has enabled over 90 percent of recipients to safely return to their work.

While we are committed to enabling the work of HRDs and CSOs as a government, this is a collective responsibility. Online platforms provide important tools and services to enable the work of HRDs. And they can do more to help them do that work safely. As companies, they have a
responsibility to respect human rights in line with U.N. Guiding Principles on Business and Human Rights.

We hope our guidance, which was developed in consultation with HRDs, civil society, organizations, and platforms – many of you in this room – we hope our guidance will provide companies with a blueprint of actions they can take to better protect HRDs. We ask that you adopt and adapt the recommendations in this guidance to improve your own policies and processes.

Thank you to our esteemed panelists for being here today and for sharing your perspectives on opportunities for continued collaboration. Collective problems demand collective solutions. And I am heartened to see so many stakeholders engaging with us today. We are all partners in this effort.

Thank you so much. (Applause.)

Ms. Strucke:

Thank you, everyone. I’m now very pleased to introduce our distinguished panelists, who will have a moderated conversation, that I will moderate, with each of them. And then we’ll have about 15 minutes at the end to have a question-and-answer session. You can raise your hand in the room if you’d like to ask a question and we have a microphone that will be coming around to you. If you’re online watching, you can submit a question and I will be able to see that question and ask it in the room, so we have full participation, hopefully, from both online and audience members here.

So, without further ado, I will introduce the distinguished panelists. So starting here to my left is Jason Pielemeier, who’s the executive director of the Global Network Initiative, or GNI. Jason leads a dynamic, multistakeholder human rights collaboration building consensus for the advancement of freedom of expression and privacy among technology companies, academics, human rights, and press freedom groups, and investors. Prior to joining GNI, Jason was a special advisor at the U.S. Department of State where he led the Internet Freedom, Business, and Human Rights Section in the Bureau of Democracy, Human Rights, and Labor. And in that role, he worked with colleagues across the U.S. government, counterparts in other governments, and stakeholders around the world to promote and protect human rights online.

Next to him is Wai Phyo Myint, the Asia Pacific policy analyst at Access Now. She has been working as a digital rights activist in Myanmar for about 10 years, and has previous experience in political advisory, media, and communications. Wai Phyo has served as one of the leading persons in Myanmar organizing the Myanmar Digital Rights Forum since it was first held in 2016. And it was – and it is and was the cornerstone for the digital rights movement.
Then we have Alex Walden, who is the global head of human rights for Google. Alex Walden is Google’s global head of human rights and free expression. She builds partnerships to promote free speech and expression and to combat internet censorship and filtering across the globe. She also coordinates policy and strategy around these issues for the company. Prior to joining Google, Alex worked at the Raven Group, Center for American Progress, and now Legal Defense and Education Fund. She also has served as a law clerk for the U.S. Senate Committee on the Judiciary and for the House of Representatives, in the Committee on the Judiciary Subcommittee of the Constitution, Civil Rights, and Liberties. And worked for the U.S. EEOC, U.S. Department of Labor, and Bay Area Legal Aid during law schools. Thank you, Alex, for being here.

And last but not least, I have Sheryl Mendez, who is the senior program manager of Freedom House’s Emergency Assistance Program. Sheryl has worked for over a decade advocating for and providing emergency assistance and logistical support to human rights defenders and journalists at risk worldwide. In her role at Freedom House, she provides support to human rights defenders and civil society organizations who are at risk due to their human rights work. Prior to joining Freedom House, she worked with the Committee to Protect Journalists, founded the Crimes of War Project, and helped launch a Culture of Safety Alliance – an unprecedented collaboration between news organizations, press freedom NGOs, and journalists to promote journalist safety. Mendez is also a widely published photojournalist who has trained journalists and documentary photographers in the Middle East, North Africa, and Europe.

So, thanks so much for this discussion today. I wanted to start with a little – couple questions to help set the stage for the participants that are watching and here in the room. So, I’ll start with Alex and then Jason with a question. You’ve worked closely with the private sector on addressing these human rights risks associated with technology for a number of years, and therefore have this very unique perspective on how companies have worked to address threats to human rights and human rights defenders over a period of years. So, what would be interesting, I think, for the audience is to know how have you seen these risks change over time? Are there private sector actions that have worked really well in combating these issues? And are there any hard lessons learned that you can share? And, you know, if you want to say, if there’s common standards today that maybe you pushed for that once seemed unachievable, really help us understand that journey of how this – the kind of situation has changed over time and how you think these guidance fit into those broader efforts.

So, Alex, we’ll start with you.
Alexandria Walden: Sure. Thanks for the question. And thanks for including us in the conversation today. It's a great question, because I think what's happened over – I mean, I've been at Google for now almost nine years. And when I look at sort of how the industry has changed, how technology has changed over that time, and sort of the way the ecosystem of civil society has coalesced around these issues. So, sort of, we're still dealing with permutations of the same thing, right? There are people who are trying to defend human rights and exercise their human rights, and there are bad actors – governments or otherwise – who are targeting them and trying to stop them from doing that good work.

So, sort of that the quintessential problem remains the same, but the tools available to bad actors have certainly evolved. And the tactics that bad actors use have also evolved. So, teams within companies have over time, I think, become more resourced to look at these things and kind of become attuned to tracking. And we've developed intel teams inside of companies that are looking at how are bad actors trying to manipulate our technology and our platforms to harm, in particular, our vulnerable users. And I think companies have also sort of made more efforts to engage with civil society to understand exactly how the problems are manifesting, and how they look different in different places around the world and – different and the same.

And so, ultimately, like, yes, there – and also, we have AI and generative AI. And these things are, again, morphing, the ways in which people are using technology to abuse rights defenders. So, all of those things are changing, and still the fundamental problem is the same, that how do we kind of collectively work together to understand how problems are evolving, to fight back against them? But it's constant, right? The threats are evolving. And so, our response to them has to evolve at the same time.

Ms. Strucke: Jason would love to hear your thoughts.

Jason Pielemeier: Yeah. Thank you, Michelle. And thank you to CSIS for hosting, to the State Department, Access Now, DFR Lab. This is – and to everyone who did the hard work to put this guidance together. I think it's really a wonderful set of principles. And I think it will have really sort of meaningful and important impact. So, kudos.

To the question, and building off what Alex said, I think it's worth taking a step back. In part, because I do think these principles really build nicely on a foundation of work that is, you know, in some ways, 20 or more years in the making. I think, for the purposes of this conversation, it's worth kind of starting with the U.N. guiding principles, which were developed in a really creative way by John Ruggie, who was the special representative for business and human rights at the time, to Secretary-General Kofi
Annan, and then sort of carried out a multiyear, multistakeholder series of negotiations that produce the Protect, Respect, Remedy Framework, which we now know as the U.N. guiding principles, which were endorsed unanimously by the Human Rights Council in 2011.

And that framework really kind of was a pivot point, in that it created a foundational shared understanding of the respective duties of states and responsibilities of companies, highlighting in addition the importance of remedy. The GNI principles were negotiated in parallel to that process. And, in fact, John Ruggie had an advisor who was embedded in the GNI negotiations. And there was a lot of crosstalk that time. The GNI principles came out of a series of incidents that were the result of persecution of human rights defenders using data that had been given to a number of authoritarian governments by U.S. tech companies. And so, the concerns about human rights defenders – I don’t think that was a term that was necessarily used at that point in time – but the sort of underlying situation of journalists and activists who were trying to use these new technologies and tools to do their work, being threatened and persecuted as a result of that, was very much what animated the GNI principles.

So we have U.N. guiding principles, the GNI principles, sort of apply specifically to the tech sector. And since then, over the last 15 years, we have seen, I think, a tremendous growth in terms of the amount of attention, the amount of resources that are put into questions around technology and human rights. So Alex mentioned that, you know, a number of tech companies now have – they have put more time and resources into this. At GNI, we have a set of principles and implementation guidelines that our member companies, like Google, commit to implementing. And then we have a kind of unique assessment process that holds them to account to those commitments.

At a very high level, those involved creating a human rights policy that applies across the company, embedding that policy through dedicated staff and trainings across the relevant parts of the company, having senior-level oversight of that work, creating appropriate escalation channels, putting in place the human rights due diligence processes that are needed to become aware of and be able to respond to human rights risks, including with respect to defenders. And then having appropriate remedy and transparency throughout. So that framework, if it sounds familiar, it’s because it’s very similar to the one that’s in these guidelines. And I think that is a really sort of helpful way to structure this, because it takes advantage of what companies have already been working on now for over a decade, and sort of hits all of those sorts of points. So that coherence, I think, will be really useful in terms of the ability of companies to take and implement this guidance. It will also help civil society organizations and advocates on the outside who are already familiar with
these frameworks be able to advocate and hold companies accountable in a more consistent way.

Ms. Strucke: Thank you. Thank you both for this really great overview of how we ended up here and how these principles are such a – these guiding principles are such an important practical step forward.

So, I want to take it now to Wai Phyo. You have such a unique perspective on these issues, having worked as a human rights defender in Myanmar and also for an organization that specifically is geared at helping other defenders. So, I’d love to hear a little bit about the context that you were working in. And then kind of if you could take us on a – sort of a hypothetical. If there were human rights defender today in Myanmar who suddenly began doing what’s happening to many human rights defenders, receiving threats, being doxed on several platforms, what steps could they realistically actually take to try to protect themselves? And then when you move to the platforms, what are the most urgent types of threats that you see that platforms need to have processes to address when you come from that on-the-ground perspective?

Wai Phyo Myint: Thank you. Thank you so much for having us today. Like, I'm here, you know, not necessarily – not just as a team member of Access Now. I’m also here as a human rights defender from Myanmar. So, just to give you a bit background, you know, for many of you, like, who might not necessarily know well about what is going on in Myanmar, basically, like, currently right now we are – I mean, over three years now people in Myanmar tirelessly resisting military coup, you know, started 1st February 2021.

But on a daily basis, what we have been seeing, like, on the ground for these over three years is this – pretty much, like, people in Myanmar are facing the worst forms of, like, human rights abuse atrocities, you know, committed by the military. So on a daily basis what we have been seen is like airstrikes you know, like, dropping bombs, you know, on these civilians areas, like, the towns. And many of the villages has been literally – like, the whole village has been wiped out, you know, after being burned down. Even, like, this morning, you know, like, when I was on the way, I received the message, you know, like, one township has been basically kind of like now on fire, and their internet has been shut down, and, you know, et cetera.

So those are the kind of, like, a daily basis, you know, what we have seen about both online and offline as well. And also, like, people have been killed, you know, like arbitrary detentions and, you know, et cetera. Those are on a daily basis, you know, we have been seeing. And when you look at about online, so, the same as well. You know, like, internet shutdown has been – military has basically shut down internet since the day one. So
currently, right now, when we are speaking, over 80 townships, that’s me, like, almost more or less 1/3rd of the country doesn’t have the internet at all.

So, some of these townships, like, they are around – like, 30 townships are – it has been over two years doesn’t have internet. And also in some areas, they not necessarily just internet and also mobile communication has been – has been shut down as well. And then, like, and also the other side. You know, like a tons of, like, websites – including all these social media and messaging platform, has been blocked. It has been almost three years now. And then even the use of the VPN has been banned in Myanmar. And then, like, at the other side, you know, when you look at about it, the military has been trying to use different tools. They are trying to do abuse or sort of, like, digital tools to be able to extend, you know, like, their surveillance hands, you know?

You will see about it there. Like, they have been abusing, you know, like all sort of data collected from, like, a study from the CCTV footage or even including like SIM card registration, data. Biometric data they collected through these, like, e-ID project, like, a unique ID project and, you know, et cetera. So they have been abusing, you know, like to be able to – all sorts of these data to be able to kind of, like, do, like, a multiple filing to be able to identify these individuals, to be able to trace, you know, where these people are exactly, and then what they are doing, and et cetera. To be able to monitor their online activities, to be able to monitor their financial transaction, you know, like – and all sort of, like, violating all their privacy then, et cetera.

So that is also – we have been seeing on a daily basis as well. And also at the same time, you know, like the military has been kind of actively monitoring you know, all these social media, because, like, even though they banned social media and also messaging platforms and et cetera, people are trying to find a way, you know, to be better connected, and et cetera. But they are still monitoring all these digital footprints happening across different platforms, and doxing people, abusing people. And we have seeing about – literally this was – like, what we have been seeing are a part of kind of, you know, the campaign of terror. You know, that’s what – basically what we are seeing. Properties has been confiscated, you know, people have been arrested, and arbitrary detention has been happened.

And even, like, a killing, like, just, like two weeks ago. You know, one of our close friends was – basically got killed after get out – because she was arrested. And then there was – on that day there was a trial. And then right after the trial, we didn’t get information, you know, where she was taken, and et cetera. And then a few days later on the way back from the
court, she – basically, she just got killed. So those kinds of information we have – we are – I mean, basically, kind of, like, you’re seeing on a daily basis. This is the level – you know, the threat level, the roots level about people in Myanmar are experiencing.

And then here we use this, like, “human rights defenders,” you know, the term “human rights defender.” But – thank you, like, our keynote speaker. He also defined it, like, human rights – the term, like, “human rights defender;” as well. But in Myanmar – majority of the people in Myanmar are currently right now, I mean, basically kind of like they are standing up. You know, they are taking the key risks, you know, to be able to defend their rights, to be able to defend the rights of their generation, you know. They basically – so, when we talk about sometimes, you know, like, when we talk about the term of the “human rights defenders” and et cetera, particularly in Myanmar, pretty much like every individuals are human rights defenders. And the risk they are having – the risk, like, the threat level, you know, they are experiencing is pretty much, like, at the same, more or less – the same level, you know. On a daily basis, they are facing it.

Like, for example, you know, even the public school teacher and also the school children, you know, who are boycotting public school system, which is under the control of the military, they refuse to attend the class. They refuse to go back to the public school. They are arrested. They are – many of them have even got killed as well, you know, just for refusing the school system, you know, controlled by the military. This is – this kind of, like, threat level. You don’t necessarily need to be a kind of, like, politician or high-profile human rights. But even on these, like, I mean, students, like, schoolchildren can be basically – you know, have been targeted, you know, and monitored. And their activities have been monitored, and et cetera.

So, the best – sorry, back to the question level. So, I am – I closely work with the local groups, who has been monitoring on the digital rights abuses and, you know, et cetera. So, we closely – this is pretty much like a small group. And that this group also, we have a kind of, like, network with the extended civil societies and, you know, like, labor unions, and the student unions, and, you know, et cetera. So on a daily basis, like, the message we receive is if somebody got arrested from any of these networks, they alert to us, because, like, they want, like, a kind of – you know, their digital footprint, like, their accounts to be taken down, and, you know, et cetera. Like, if that person has a Facebook account, they want to secure the Facebook account, Facebook page, Telegram channel. You know, and even if they have a Gmail, you know, like, they would like to access it.
So, basically, this is the kind of, you know, like, messages, you know, on a
daily basis we receive. You know, whoever, like, from this network got
arrested, they alert it to us with their URL, you know, sort of, you know,
can you please help us, you know, secure these accounts, and et cetera?
So, that was – like, we basically kind of, like, collaborate with the others
digital rights group, and also Assess Now, and also a helpline, and also
collaborate with these, like, different platforms, and et cetera.
So, those are basically kind of, you know, like – I will say about it, like, a
step, you know, but not necessarily kind of mitigate the risk. You know, to
mitigate the risk mean, like, only we basically kind of, like, took these
steps, you know, only after somebody got arrested, we got notified, right?
To be mature about it, they are kind of, like, digital communications has
been secure and also the network, you know, the involved and, et cetera,
are secure, and et cetera. So, those are kind of like the immediate steps
that we have to take it, right?

The other one are basically kind of, like, we collaborate, like, our
organization and also, like others, the digital rights organization, we
closely work. So there, will also work around on the mitigation plan as
well. You know, that is also some of what we engage with these different
platforms, you know, to make sure about it. Like, we can be able to kind
of, like, foresee, you know, what are the risks and what are the mitigation
plans to be able to inform these, like, human rights defenders, and also
media, journalists, and, you know, et cetera. So basically, those are kind of
like a day-to-day work, you know, we have to take. And also this is also,
like, lead off, like, a collaboration with these, like, the stakeholders,
including the – like, including the platforms as well. Thank you.

Ms. Strucke:

Thank you so much for your work, for the work of the human rights
defenders that you are in contact with that are facing these conditions
every day. It was so powerful hearing what you just said, because you had
in it both the fact that authorities block the internet, which is a lifeline to
people and means defenders can’t access tools that they need. At the same
time, isn’t that an indication of how powerful it is as a tool for human
rights defenders? So I heard both of those in your statement.

And then the idea that it’s used – these platforms are used to track and
monitor people, I think it really raises a good question for you and for
Sheryl about this reporting – these secure and accessible reporting
channels. I know it’s extremely complicated because even when someone
takes a step to send that message in something that could be monitored,
they’re putting themselves at risk. So how – are there lessons that
Freedom House and Access Now can share with platforms on the steps
that they can take to develop these secure and accessible reporting
channels, which will support human rights defenders when they’re facing
harm in the places that they’re defending human rights? So maybe I'll start with Sheryl.

Sheryl Mendez:

Sure. I think, you know, one of the steps is to consult and co-create with defenders and others who are affected. That would also speak to accessibility issues, right? So, you know, when a platform understands what the operating environment for a defender is, how they’re able to access any type of channel, but also when they’ve accessed channels in the past to report abuse, or abusive language, or threats, have they gotten a response? You know, defenders and others are trying to understand – and there should be greater education and training – about what is the lifecycle of reporting? What will happen if a defender, or anybody, does report something? You know, what are the stages? What can they expect?

Because often what happens is that defenders and others, you know, they experience what American Bar Association’s Center for Human Rights, and many others, have said is, like, flagging fatigue. You know, so that’s overwhelming. And also, when they’re documenting these threats if there was greater information on how to document threats, what to document. And also across social media platforms and companies, if there was a better kind of, you know, approach where if a defender is attacked, including across multiple platforms, is there a way that the reporting process can be streamlined so that they’re not starting from scratch every single time that they may be, you know, reporting something to one or the other of a channel.

This is also really important, because, as we all know, you know, from both defenders at risk and others, that when something happens offline and then if it goes – when it happens online, and if it goes offline. And if it also leads to the criminalization of defenders or different types of legal harassment because of these, you know, orchestrated campaigns to defame them, discredit them, both in the public eye. You know, when that happens, whether governments or other actors can use that to then bring these frivolous and worse suits against them, or to charge them, or to jail them. You know, which also takes them out of their human rights work. It affects their families. You know, the costs are, you know, extreme. depending on, let’s say, if it’s legal action.

And also, you know, even with legal action, the life of a case, even if something gets dismissed, you know, those costs and the psychosocial impact, you know, is tremendous. And again, it has consequences for their family members and others. I think it’s very important for – with having secure and accessible channels, that people know where the points of contact are, offline and online. Because, for example, there may be defenders who don’t have an online presence, you know, who are still
attacked online – whether they’re indigenous defenders or many other defenders.

And if there isn’t an understanding of, like, what are the clear channels? Who are the actual points of contact? You know, if a defender is going to be able to report, then are they able to have contact with human beings, you know, who are trauma-informed, who may be able to give, you know, kind of real-time response or, at least, help them to understand what are the steps, you know? And, again, how they’re documenting, things like that. That also includes the need for resourcing, you know, local and national networks and civil society organizations. And training of trainers. Again, because, you know, with the way one reports and how they document, when defenders and others are going through this entire process and effort, and they’ve already been put under, you know, really difficult psychological strain and stress, and – you know, and threats – you know, every type of threat that’s been described.

You know, defenders are reporting to us when they’re asking for emergency assistance, or to other networks because we don’t work in isolation. You know, a defender is a land, environment, indigenous rights defender, you know, a journalist, et cetera, there are a variety of different networks. But one of the things that we and our partners do, is that we’re trying to bring those networks across, you know, in the same spaces. You know, it’s both for the reason that it’s, you know, it’s very difficult when you’re constantly contacting different types and different sources and all of that for help and to kind of work together to provide support for defenders. But because each one of these areas in the broad diversity of human rights work, you know, it literally is cut and paste.

I mean, I used to work at the Committee to Protect Journalists. When I came into working in more broad on human rights defenders, it was the same thing. It’s, like, they’re using the same tactics, you know, the same approach. Like you’d mentioned, you know, like, it’s the same scenario, except the tools and other things are more insidious, quicker, you know, you name it. But I think it’s also important for social media companies and others, all of us, you know, to understand when defenders take kind of preventative measures or precautionary measures, which includes self-censorship, right? Which includes leaving, you know, including into exile – you know, leaving the human rights field in its entirety sometimes.

And I bring this up because it’s important because that will inform how you, you know, think about safe and accessible secure channels. Because it depends on that – how you respond, you know, what is the manner of response, how quickly or efficiently, you know, and all of that. But if there is no response, then this is what happens. Defenders leave. You know, that’s a problem. And also with their families, because often, as was
mentioned, I mean, the families are attacked. You know, they’re threatened with kidnap. You know, and it’s not just threats. Like, we’ve seen, like – I mean, I’ve literally been working in this field, between CPJ and Freedom House, for, like, 12 years or more, right? And, you know, threats of abduction happen. Everything that everybody said, including the keynote speakers and all of that, like, I can name, you know, every single person that we’ve dealt with, and what country, what context, you name it, where these things are happening in, and how it’s evolved in the way – in the way it’s happening as well. As you’d mentioned, you know, the evolution.

One of the other things about accessibility is, you know, including, you know, for example, persons with – sorry – with disabilities, and defenders who are working in this space as well, and other marginalized communities, when you’re thinking about different reporting channels and how a person would access them, you know? And then I would also say that – there was – oh, one of the things that defenders have brought up, you know, and I think it’s really important and I wrote it because I want to make sure that I express this. But they want to understand and they want guidance from social media companies, and protection groups, and all of that, that – for example, if they experience online abuse – hateful speech, et cetera – what do they do if they block speech or they mute speech, you know, or they report threats when they’ve seen, for example, sometimes when they blocked it that threats accelerated or escalated, right?

When they’ve muted it, you know, then they may not have access to something that they need to monitor in order to document and report what’s happening. And then also, you know, when they report threats if they don’t receive a response, you know, then what did they do if, in fact, it takes time and they won’t receive a response in a manner that they would need or in time that they would need? But there could be advice. This is some of the things that you can do, right, along the – along the process. And it’s also again, I mean, about training and resources, because often defenders who are subjected to these type of threats, and hate speech, and things like that, you know, they may need colleagues and other trusted, you know, people, you know, in their networks to monitor these things for them, right?

So they need this kind of education, you know, and these trainings, and trainings of trainers. You know, it’s almost like everything that, you know, Access Now and other groups in the protection landscape – whether they’re frontline defenders or American Bar Association’s justice defenders or many others in all of these different networks – the processes and things that have evolved in these networks, including working collectively, you know, that’s something that social media
companies are going down that road. But there's a lot to learn from what
are the lessons from these networks, and particularly at the local and
national levels? And also consider when defenders may be not near
capitals but are in remote situations, what are the challenges, then? You
know, if they're deep in a context where they may be at risk? You know, so
I'll just – that was a mouthful.

Ms. Strucke: Thank you. I mean, you presented such a rich picture of the tensions that
people are facing when they're trying to report, and the networks that are
supporting them. And the kind of common theme I heard was certainly
the idea of having common processes from the platforms to be able to
understand, well, who's the point of contact to go to, and online and in
person, what do they do? I want to ask Wai if you wanted to add anything
to this picture, especially when it comes to what platforms are able to
actually do that human rights defenders on the ground need that would
help them as they try to do this?

Ms. Myint: Yes. Definitely. I agree with, like, the channels, you know, like, a contact
point and et cetera. Those are quite essential. Especially, like, the issues,
you know, like, human rights defenders on the ground are kind of, like,
changing, you know, like, quite constantly. And also from one country to
another, the risk level. And, you know, like it the situations are quite
different from one country to another. So, that's why, like, I mean, kind of,
like, the platforms, you know, like, they have a global policy and, you
know, like, one policy fit for all. And, you know, et cetera, it doesn't really
work, you know, in reality.

So, like, that's why, like, we actively encourage, you know, all the
platforms to engage with a local – like, a CSO local activist and, you know,
to be able to first identify the risk level, and also to be part of the
mitigation plan, right? So currently, right now, to be honest, we have even
in Myanmar it's a – I would say about it, like, because we have not
necessarily just rearrest, or even, like, a kind of since last decade, you
know, we have a number of issues – like a hate speech, you know, like a
genocide, and, you know, et cetera. So that's why, like, we kind of – I will
say about it – like, got some sort of, like, international attention, and also
attention from these different platforms, and et cetera.

But still, you know, like, I will say, like, we have very few platforms, you
know, who are regularly engaging with the CSOs on the ground. So that
definitely need to change. And also, the thing is – like, and also the other
thing, like, what we have been seeing about it, like, normally what the
platform usually do is more about kind of like addressing the kind of, like,
threat, you know, like, they are experiencing, the human rights defenders
on the grounds are experiencing, et cetera. Oftentimes, you know, we
don't really see that much, you know, like a proactive approach part of
this, like, mitigation plan, right? So, that is also definitely the area we would like to see, like, much more progress as well, you know?

And then, like, the other one that even one of the recommendations about, like a change of, like, information, you know, that I hear about it, and also quite key as well. Like, for example, you know, like, we exchange information, you know, often time to time. You know, when we trying to engage with the these different platforms, you know, legal organization, you know, they all – like, who has been monitoring online content and, you know, et cetera, they flash these issues. You know, oh, these are the bad actors. These are the issues. These are the kind of, like, links and, you know, et cetera, right? They say the with the – but they also have a limited capacity as well.

But sometimes, you know, like, at this – the information flow is always kind of, like, one-sided, right? Like, we fill this information in, you know, we get this information in. But oftentimes, you know, we don’t really know where this information is going. It’s literally kind of like a drop in the black hole. And how this information will be kind of, like, get taken into the consideration behind the platforms. You know, how the – how this information will be kind of reflected in the policy change. And, you know, we don’t – we don’t have these kinds of information. And also, often time to time, you know, we don’t really see that kind of, like, reflection as well.

So, and also at the same time, like, they are a lot going on. Like, the different platforms that they have, like, they are kind of, like, investigations and, you know, et cetera. So I think, like, these kinds of, like, exchange information with the CSOs, you know, what they see on the ground and then what the platform are seeing on that their platforms, and, you know, et cetera. These kinds of exchanging information I see about it, it will be, what, like a regular basics of exchanging information would be quite useful, especially for the CSOs who are working on the protection part, like, including digital security, and, you know, physical security, and et cetera.

At least they can foresee, you know, what is going on on the platform as well, who are the bad actors, you know? Sometimes, you know, these bad actors are not necessarily within their own country territory, right? They have links to Russia. They have links to China. You know, they have links to these other countries, and et cetera. This, you know, like a platform have this information, right? So CSOs, local organization who are working on the ground, having this knowledge, having this information is, what, kind of, like, I’ve seen it helpful, you know, in their consideration, in their – like in educating, you know, their network, their public, and et cetera.
So, I will say about it, like, we also would like to see about it, the more kind of, like, a(n) exchange of, like, the information in the future as well. Definitely, like, a regular engagement. I think that’s kind of like a pretty much like solved. Most of can be able to solve, like, most of these issues, yeah.

Ms. Strucke: Well, thank you. I want to definitely get to, you know, some of the really important questions that you’ve raised, and give Alex a chance. If you – maybe you could help walk us through a little bit of, you know, from an example of a platform, how do you look at these reports when they come in? Kind of what do the processes look like when you think of what message you want, you know, human rights defender to hear about how Google does it? And in that sense too, how do you – what factors go into deciding how you kind of structure protection mechanisms? That behind the scenes might be really helpful for people to hear.

Ms. Walden: You know, I know this is something we have long talked about. I think there is a lot more work to be done between the platforms generally and what information sharing mechanisms might look like. There are obviously lots of challenges around privacy, and security, and our ability to validate information before we share it out. But obviously, we know it’s useful to those who are working on the ground. And so certainly lots more opportunity to think about what’s possible in that space.

But sort of just to back up and talk about sort of how we think about these issues and how it sorts of fits into the structure of the company – because, to Jason’s point, like, it’s a big global company with a lot of people and a lot of teams and a lot of product surfaces. And so how do we make sure we’re paying attention to the issues that are coming up in Myanmar, across Latin America, across all regions of the world, right? So, I think, first, it really – like, we do have to focus on security by design.

And that means that our teams that are focused on looking at threats and understanding the threats that are coming at our platforms all day every day are informing how we are building all of our products. Because at base, like, in a perfect world, our – the way that you flag an issue in a product that any user around the world would flag an issue would also solve the problems of our most vulnerable users. And when you design for the most vulnerable users, then you’re also solving problems for everyone. So anyway, that’s sort of why security by design is so important. And I think why when we do that it sort of helps us get a little bit closer to solving these problems.

But obviously, like, in addition to building security into the products at their foundation, we think about what are the specific features that some particularly vulnerable users might need. And so that looks for us like in-
product features. Anybody that has Gmail might have received a notice that says: It looks like you might have been targeted. And you’ll get a notice from us that says you may have been targeted. We may not have a lot more information we can share with you, but that’s a flag to someone that they might be being targeted, one. And then we also provide them with some links about ways to check the security on their account, and some other resources. So, making sure that people have resources to do some of those checks themselves.

And then we also spend time thinking about specific products that might be useful to groups that are being targeted online. And so, we have things like the Advanced Protection Program, which is a super secure version of Gmail that lots of – that we sort of have engaged with journalists and rights defender organizations, as well as sort of, like, candidates that are running for office, because we know they are also likely to be attacked. So, making sure that those – that those groups of folks have access to this tool. And it’s not just sort of individual accounts, it’s also sites. And so, we have a program called Project Shield where we provide additional security to sites that might be subject to DDoS attacks or other things like that. So really investing in additional tools that we know people might need.

And then, you know, obviously, engaging with stakeholders is something we have to continue to do to make sure that we are understanding how the threats are evolving. And that needs to feed into the structure, the programs, the process, and the teams across the company that are working on these issues. And that really runs the gamut, again, from engineers and product developers, to trust and safety who are writing the policies and enforcing the policies, and our public policy teams who are doing advocacy around things like fighting internet shutdowns and making sure that there are adequate protections in place around censorship and privacy. So that – sort of companies need a comprehensive approach. And it has to be built into the way you build products, and then also that you have processes and policies in place.

And then, of course, having particular mechanisms for rights defender groups to come directly to your human rights team. Companies should have the human rights team. And when they don’t, that – it doesn’t make it perfect, but I think if you don’t have that, it sort of means that you don’t even have a way for the company to begin to understand how they have a responsibility to address these issues, and kind of just start thinking about how to do that in concert with other stakeholders.

Ms. Strucke: Thank you for that really fascinating answer. And it’s definitely a lot to think about in terms of how big of an issue this is across how many
countries, including here in the United States, and how you have to respond.

I wanted to ask Sheryl a little bit about some of this question on kind of, as we’re thinking about what platforms do, need to do, what kinds of teams and human resources they have in place, some of the most dangerous threats to human rights defenders often rely on this coded language or images that basically might bypass detection from automated systems, or even human reviewers who lack the knowledge of local languages, context, slang, symbols – things that people can’t find if they don’t have that very localized information.

So, Sheryl, can you tell us more about how you’ve seen this issue arise in your work with human rights defenders around the world? And then specifically, how can platforms you know, taking what Alex said about needing to communicate more with stakeholders and engage different teams – how can they engage civil society and others with that kind of contextual knowledge to build that up? And then, you know, bring it into, I think, not just the human rights teams but also, as Alex mentioned, people designing products and features for companies?

Ms. Mendez:

So coded speech, whether hate speech or otherwise, is very contextual. And one of the things that’s really important, as has been said, is that companies have a physical presence, a field presence, or they also have teams on human rights but also linguistically, teams that understand historical narratives, historical violence, you know, teams who also understand and can monitor political language and political histories, cultural, et cetera. Because one of the things is that – one of the difficulties is when speech doesn’t seem direct, that it’s a direct targeted attack, then often not only it doesn’t get reported, but it’s not seen as something that could lead to offline violence or other types of violence.

And without understanding the local context, without understanding language and how it’s used, you know, and different expressions, you know, or different allusions to – you know, without that then there is an understanding of, like, this is a direct threat. And also, often this use of indirect, you know, types of language – like basically talking about the longevity of a defender’s life, saying that something should be done, wishing that something would, you know, befall them, talking – dehumanizing them. I mean, we’ve had many reports from defenders where they’re basically not considered human, first of all, that they’re a virus, et cetera.

You know, but again, referring back to in some contexts language that’s been used historically during political violence, for example. But also, you know, on language where defenders, you know, it may call into question
their gender, you know, language, which also, you know, accuses them of corruption and criminalization, or belonging to different criminal groups and things like that, because that also then leads to threats in the legal sphere, jailing, you know, things like that. But also, on the other part – to your question about how platforms can inform, you know, and build their contextual knowledge. I think the thing is, as has been mentioned, I mean, cross-functional, interdisciplinary, different types of teams.

And also, you know, kind of focusing on an abuser approach. Because defenders – you know, that’ll kind of decrease the burden that’s on defenders for them to flag and – you know, flag content, et cetera. But it also – because of the phenomenon we were talking about earlier, about flag fatigue. You know, so, but I think that, as was mentioned, besides having human rights experts, having, you know, people who are experienced in journalism and political contests, that also helps to unearth some of these type of nuanced threats or coded threats. But also, you know, getting away from these kinds of standard lists of hate speech, right, or certain types of vocabularies that are used. As was said, you know, it’s not a one-size-fits-all.

So, there are different types of known speech that may be considered hate speech or otherwise. But if we just stick to those, then we’re also dealing with speech which might be invisible and not measurable, you know, because we don’t even know it exists. But within the local context, defenders and others do know it exists. And they also constantly flag it. And it’s not seen, again, as, well, that doesn’t really rise to the threat level of a direct threat. But in that context, it does, including, you know, what defenders are called.

In certain contexts, if a defender is called a criminal, you know, or an enemy of the state, or a variety of other things, you know, that is, you know, a means that often these orchestrated or kind of campaigns against them, you know, get activated. And then the Catch-22 is that defenders and others are so overwhelmed by the number of – weather posts or whatever it is – that not – you know, one individual can’t reasonably, you know, handle that, never less report on it. You know, so that’s –

Ms. Strucke: Yeah. Well, thank you. I think you’ve really raised such important points for platforms to consider. And hearing a couple of themes in that. Hearing the need for that very specific human rights defender, localized community-level engagement. And perhaps you’re mentioning with people that are actually marginalized themselves, vulnerable people. I know that even in the U.S. context, you may have a majority group that – like you said, they can list names of common hate speech indicators. But they don’t experience it themselves every single day in a way where they understand exactly what that insinuation means, or exactly what that
symbol or kind of allegory or allusion means. So I think that I’m hearing that. And also an opportunity for platforms to look at those patterns in reporting to figure out what is not rising to the level, but maybe is exposing an emerging trend. And that’s something it sounds like they need local people to help navigate. So, yeah, go ahead, Alex.

Ms. Walden: I just wanted to chime in because I think, like, certainly at Google, this is something that we are deeply invested in. We have – our trust and safety team is global. And they are – they do exactly this. They sort of – for our hate speech policy in particular – they are looking at what are hate terms, what are thematic narratives that are coming up in the hate space, and how those evolve, and trying to make sure we have taxonomies that are keeping up with the ways bad actors are dehumanizing and inciting violence, et cetera. So, like, but it is a huge investment for companies. And, you know, I see my colleagues from Meta in the room. Like, they do the same thing.

And I think one of the things we need to think about are ways to resource the diversity of the industry, because it is something that certainly the big companies are invested in – and could improve, but are deeply invested in. But how do we make sure that smaller companies that can have a really big footprint are getting access to this type of – sort of intel from experts about what narratives – what narratives exist and how you should interpret them in a particular context? That takes a lot of people resources that not all companies – in particular, small companies don’t have yet. So I think that’s an important kind of, like, ongoing challenge for the ecosystem.

Mr. Pielemeier: Yeah. Thanks, Michelle.

So, this has been a really, really rich conversation. And I think the question of how do we sort of take this forward and measure progress is a really important one. So GNI has a framework. We’ve been – for 15 years. So we’re a multistakeholder organization. We have tech companies – not just sort of internet companies, but also telecommunications companies, cloud providers, infrastructure providers – all of whom sort of interface with free expression and privacy slightly differently, depending on the products and services they provide. But all of whom have obviously, by virtue of being part of GNI, made a commitment.

And that commitment sort of is broken down in the principles and our implementation guidelines into these kinds of specific measures. And then we have a periodic assessment process that each company goes through. And in that process, that company will bring in an independent third party, which we accredit, to review the steps they’ve taken against each of the categories of obligations, and document that. And they do that by
looking at the sort of internal paper trail of, you know, what systems and policies are there. Not just the public-facing ones but the internal ones. They talk to key employees from sort of senior-level management all the way down to the people in the field who are kind of interacting with and dealing with threats on a daily basis. And then we look at case studies. So actual examples of how free expression and privacy challenges manifest. And, you know, we place particular focus on the interaction between companies and governments, because that’s where a lot of these threats manifest.

So, all of that goes into a report, which then is shared with our multistakeholder membership for review, discussion, and recommendations. So, we evaluate companies against the benchmark, which is good faith implementation with improvement over time. And this cycle repeats. Recommendations that are provided to the companies then are reviewed at the next assessment in order to make sure that there is progress happening. And so that improvement over time concept, which is also baked into this guidance, I think is really critical. But having a concrete framework and process to be able to measure improvement is really important. And improvement, of course, can mean lots of different things.

I think what’s interesting today is the fact that we are now seeing a number of emerging laws and regulations that are effectively taking a lot of these recommendations and guidance from the U.N. guiding principles, the OECD guidelines, and baking them into hard law. So we have things like the Corporate Sustainability Due Diligence Directive, which is in the process of, it seems like, passing in the EU. (Laughter.) Which applies to all companies of a certain size with certain presence in Europe, regardless of sector. And that basically is a mandatory human rights due diligence law that will require covered companies to conduct human rights due diligence and demonstrate how they are doing that, how they’re addressing the risks that they uncovered through that.

Then we have tech-specific regulations, like the Digital Services Act, which apply in particular to segments of the technology ecosystem. And there are obligations for all kinds of different companies. But the very largest online service providers and search engines have to go through a pretty rigorous risk assessment process. And they have to have that audited by a third-party auditor. And so there are sort of these elements of the human rights – Business and Human Rights Framework that are now being codified. Which hopefully will mean that not just the very largest providers, many of which are members of GNI who’ve kind of already been doing this through a framework of sort of co-governance, but also the smaller providers, the providers who haven’t committed as much to human rights as a policy or as a practice, will now have to sort of raise
their game at least to a sort of minimum level. And over time, hopefully that that floor will rise.

A lot of questions about how this is going to work in practice. We can get into that if you’d like. I do want to say, I think there’s – just taking stock of a lot of the conversation, and knowledge, and experience that’s being shared here. I think when we think about human rights defenders specifically, it may be helpful to kind of understand that there’s sort of two types of defenses, or actions that companies can take to help defend against attacks. Wei Phyo really, I think, poignantly pointed out how in Myanmar basically the entire civilian population has become human rights defenders, right, in one way, shape, or form. And so their individual account actions or not – there’s no way you can sort of do that for every single person using a service in Myanmar.

So that’s where it’s really important to have kind of general corporate practices that can protect against threats. And I think there is none more important in that context than end-to-end encryption, which is, you know, a vital security and privacy measure that, fortunately, we have seen tech companies like Google and Meta taking steps to sort of mainstream across products and services. You really cannot underscore enough how important that can be for not just the sort of explicit human rights defenders, but just everyday people who might find themselves from one day to the next becoming a target.

And, you know, that’s not been – it’s not sort of an obvious thing, because there are a lot of governments and law enforcement agencies who see end-to-end encryption as an obstacle. Not just the authoritarian ones, but even democratic ones. So I want to just underscore that. And I think in general then cybersecurity and information security, security by design measures, right, these are things that can apply across the board addressing threat actors, right? And a lot of companies have been putting time and energy into understanding these threats because they’re not just bad for individual users, but they’re really bad for the product and service if they become, you know, so pervasively influenced by these threat actors.

So that’s the general level. And then we have the kind of specific projects, or programs, or mechanisms that can be made available to people who are known activists and known targets, right? So that’s – like Alex was talking about advanced protection and Project Shield. And there are a bunch of other programs like that. And I think those are – those are really important for these specific actors, but they’re never going to be available, or useful, or even really relevant to the general population.
So I think as we think about measuring progress over time, it’s worth looking at both the kind of systemic sort of efforts that companies can take and how those are progressing and how we’re learning across the industry and across stakeholder groups about their impact, and then the specific measures and how some of those might become not just sort of specific to a particular company and a particular user, but can we kind of think about ways that, across the industry, these protections can be provided more consistently. Because it was pointed out, I think really appropriately, that these threat actors don’t just play in one space, right? And the threats migrate, as do the users, across different platforms.

Ms. Strucke: Thank you. And I appreciate how you talked about both sort of the systemic benchmarking level of companies of their realization of improvements over time, but also, I think, from the kind of activist or on the ground perspective, people can feel quite impatient for that gradual realization to happen. So I also appreciate that you talked about concrete things, and so did Alex, that are proactively happening to be able to address these.

So, in the interest of time, we’ll definitely turn now to some audience Q&A. If you have a question in the room, please raise your hand. I will start with the first one online and that way it gives you also time for more people to raise their hands because they know sometimes there’s a first-person effect of someone’s being shy. So I’ll start with a question from online that we received.

You know, is there anything specifically around gendered online harms that’s recommended? Especially given the outsize harm faced by women human rights defenders? And the U.S. also just launched the National Action Plan on Business and Human Rights. And I also heard people discussing the fact that again, gender, isn’t kind of specifically called out. Obviously, there’s many vulnerabilities that would cause a person to be – have this outsized harm, and gender is just one of them. But I was curious if there’s any, you know, anything specific on gender that anyone wanted to share about the guidance that could be applied to platforms?

Ms. Mendez: I think, considering when someone is attacked because of their gender, also, that they may be attacked because of their families, or their families may be attacked. What are the protective mechanisms that already exist, for example, through social movements, you know, that work for the protection of women and other marginalized defenders who may be attacked because of their gender, or because of hate speech, remarking about their gender, or otherwise? So I think that these – that it’s really important to look at, like, who is working within this area. Because they’ve also had a lot of experience on what, you know, gender-specific
attacks, and threats, and protection, and mitigation, and all that, looks like.

Because it’s also not something new. I mean, women and women who identify – people who identify as women and others who are marginalized, you know, a lot of this is already down the road quite a way. You know, but again, you know, the threat actors are using different means to go after them. And in many cases, they go after their families. And on support, you know, like, let’s say, if somebody needed to relocate for their safety because of threats, often some protection measures don’t work because it doesn’t consider their family or other people around them who may be at risk. But also, you know, protection also includes when someone may be at risk from their family, because the impact of threats on them, or from their community, or otherwise.

Ms. Strucke: Thank you. And I think it’s really important for, as we’re discussing this, as people think about the fact that these threats can emanate, you know, unlike in a physical threat where someone’s right in front of you, from really anywhere. And they can affect people that are in the person’s family and network, in addition to themselves. So thank you. Those are great points.

Ms. Mendez: Sorry. I would just also add the psychosocial impact. You know, because often, you know, the threats also speak to denigrating the person, you know, and their reputation, and calling – you know, for example, if it’s threats against a woman, calling into question, you know, her womanhood, or being a mother, or otherwise. So, again, I think psychosocial – both in remedy, in responding and understanding the impact that this has on a person besides the fact that they may, you know, not be able to navigate online or otherwise because of threats. But just, like, literally from, like, every sphere close to a person – themselves, their family, friends, like how it goes out, their society, et cetera – how this may impact those different relations, and how they can navigate, including offline in the physical world.

Ms. Strucke: Well, thank you.

I’ll turn to an audience question. Please identify yourself and ask your question. I’ll start with you. And take a microphone from Elliot. Thanks.

Q: Lisa Poggiali from USAID. Thank you so much for this panel. It’s been really wonderful, and instructive, and rich set of conversations. And really excited about the guidance as well.

I wanted to go back to something that, Sheryl, you said earlier, which really struck me, about the lack of coordination between platforms on the
ground and how that affects human rights defenders. I’ve been traveling to different contexts over the course of the past year, and it’s struck me that in certain spaces civil society organizations will say, oh, we have a great relationship with YouTube. We have direct channels. But Meta we can’t get on the phone for anything. And in other places, it’s like, oh, we can talk to, you know, TikTok, but, you know, we can’t talk to Google, or whomever it is.

And so, the lack of sort of coordination in different spaces is just so apparent. And across different geographies. And, to Jason’s point about, you know, when there isn’t coordination then threat actors will just migrate. And so, the threats will migrate to the platforms where there’s the least amount of protection. So, the question being really for Alex mostly, is to what extent are there conversations being had among different platforms about generating some kind of more streamlined approach? And also, to the point about resourcing, right, it seems like that would be smarter from a resourcing perspective to cooperate with one another on the ground. And what are some of the barriers that you see to that happening?

Ms. Walden: So I think – so there’s a lot of conversation that happens among the companies, in particular the GNI companies, around how do we learn from one another’s best practices about how we’re engaging with intermediary organizations and with organizations on the ground, sort of, in particular localities or globally, and what programs we have to do that, and kind of, you know, our best practices around implementing those internal guidelines.

Some of the things, I think, that are ultimately, like, some of the barriers to more coordination are the platforms aren’t necessarily similarly situated in any given country, right? So, the user base, the company’s sort of market share, et cetera, all those things look really different. And then the way people are using our platforms can look different. And so, we won’t always sort of have the same amount of resources, or energy, or approach to put into something at a given time. And obviously, as we’ve talked about, like, that can certainly evolve.

And things that might be a priority at one time might become less of a priority as the situation changes, or as our user base changes somewhere. But that just is the reality of how and why it might look different for different companies in a particular country, because our services just aren’t being used in the same way. And so, our approach to managing the issues might look a little bit different.

Ms. Strucke: Well, thanks. We are unfortunately at time for this. And I want to let you all get out of here. I felt a palpable sense in the room of how many
questions I think we wished we could have asked. I have definitely a few more here online. I want to thank all of our panelists for all the work they’re doing from each place they sit in advocating for greater protections for human rights defenders. I want to thank the State Department for releasing these really incredible, concrete recommendations for online platforms for protecting human rights defenders. And of course, to thank the Atlantic Council and Access Now as well for their support and partnership of this.

We will be continuing these conversations. These are important topics. So you can always contact us at the Center for Strategic and International Studies. We’re the Human Rights Initiative, if you want to see more of this kind of content, if you have more questions. But it’s certainly an important issue that affects people from the bottom all the way to the top of our society in terms of decision makers and those that are on the frontlines of fighting for human rights. So thank you, again, for coming today. Please join me in thanking our panelists and our keynote speakers for a great session. (Applause.)

(END.)