# Briefing :: Online Safety Under Repressive Regimes: What is the Responsibility of Technology Companies?

Commission on Security & Cooperation in Europe: U.S. Helsinki Commission

Online Safety Under Repressive Regimes:
What is the Responsibility of Technology Companies?

Committee Member Present:
Shelly Han, Policy Advisor for Economics,
Environment, Technology and Trade

Witnesses:
Amol Mehra,
Coordinator,
International Corporate Accountability Roundtable

Susan Morgan,
Executive Director,
Global Network Initiative

Meg Roggensack,
Senior Adviser,
Global Network Initiative

The Hearing Was Held At 10:00 a.m. EDT in Room 2203 Rayburn Office,
Washington,
D.C., Shelly Han Moderating

Friday, October 19, 2012

SHELLY HAN: All right, good morning. On behalf of Chairman Smith, the chairman of the Commission on Security and Cooperation in Europe, I'd like to welcome you to today's briefing. I know it's somewhat trite, but it's still true to say that the Internet has opened tremendous communication and advocacy avenues in a truly revolutionary way, but it's also true that the Internet has also revolutionized the way governments can monitor and know even more intimate details about their citizens with very little cost or effort. If you haven't seen it, I want to recommend you to see a movie called "The Lives of Others," – and most of you I see in the room are probably too young to remember the Cold

War, but the movie portrays really accurately the old-fashioned way of surveillance, where you had teams of people that were dispatched to listen in on phone conversations and follow people around – and now with the Internet and GPS, it's so much easier for governments to get that information with much less manpower and expense.

And when you pair that with a government that does not respect human rights or where citizens don't have the ability to assert their own human rights, then it's truly a dire situation. The chairman of the Helsinki Commission, Congressman Chris Smith, introduced the Global Online Freedom Act in order to give more power to those who are living in just such a dire situation. The Act really isn't aimed at protecting users in countries where we have the freedom and abundant opportunity to lobby our governments and where we have an independent judicial system in which we can wage legal battles to – for our own rights, but it is aimed at giving a voice to those who don't have a voice in their own country. The Global Online Freedom Act envisions a reporting requirement for listed U.S. companies.

The issue of corporate responsibility and accountability is critical since the Internet that we use every day is run by private companies. The business model of most consumer-facing websites means that they collect whatever data they can from your online activity and then use that data usually to sell advertising. But because this data is stored for often unspecific lengths of time, this potentially puts consumers at risk to either hackers or government agencies who want to access that specific information. The question of how companies treat user data painfully came to light when it was disclosed that Yahoo had given the Chinese government information that confirmed the identity of Shi Tao, a journalist who was subsequently imprisoned under the charge of revealing state secrets. Shi Tao is still in jail in China.

In many ways, that incident several years ago sparked some of the first debates on the responsibility of companies to their users, particularly when those companies are working in repressive countries, and that's what we're going to be focusing on today. And what we're going to do is look at where we have come since the early days of the Internet and where we're going in terms of corporate responsibility. The panelists here are all experts in the field, and I look forward to hearing their views. I'd also like to invite the audience

to
think about questions that you may have, because during the question and answer
period, we will open it up to the audience for questions since this is a
briefing and a little bit less formal than a hearing, so I'd welcome your input
and questions at that time.

So first I'll turn to our panelists; we're going to go in alphabetical order,
so we're going to start with Amol Mehra, who is the coordinator of the
International Accountability Roundtable. I have – we've distributed the bios
for each of the speakers over on the table, so I won't go into those, but I'll
let Amol get started. Thanks.

AMOL MEHRA: Well, thank you, Shelly, and thank you to Chairman Smith and the
members of the Helsinki Commission for conducting this briefing. The
International Corporate Accountability Roundtable is a coalition of leading
human rights environmental development groups and unions. We work to build
robust frameworks for corporate accountability, to strengthen current measures
and to defend existing laws, policies and legal precedents. So as Shelly
mentioned, the Internet and communication technology companies are increasingly
acting as mediators both for access to and content of information, placing them
at the forefront of discussions on corporate accountability. This is most
evident in the context of oppressive regimes, where controls or restrictions
over the Internet are commonplace, and effectively turn a tool for advancing
democracy and freedom into a means of censorship and surveillance.

Businesses should not be complicit in such human rights abuses. We believe
that any effort to tackle the responsibility of the ICT companies vis-à-vis
human rights must include a clear requirement for these companies to conduct
human rights due diligence. This is consistent with recent regulatory
approaches in addressing corporate responsibility for human rights, including
the transparency provisions of section 1502 of the Dodd-Frank Act pertaining to
conflict minerals and the due diligence policies and procedures contained in
the reporting requirements on responsible investment in Burma issued by the
U.S. State Department in 2012. Governments, as primary duty-bearers of human
rights, must therefore take regulatory action to ensure that companies respect
human rights, including by imposing binding requirements on companies to
conduct human rights due diligence. Strong, effective human rights due
diligence procedures are fundamental to ensure that human rights are respected
and company actions both inside and outside the territory where they are based,
and governments should mandate independent monitoring in appropriate cases and

public reporting of companies' human rights impacts to verify their compliance.

These requirements should cover all business relationships, including suppliers, including contractors, security forces, business partners and recipients of finance. For this reason, ICAR has supported the Global Online Freedom Act, or GOFA and the disclosure requirements regarding human rights due diligence policies contained therein in Title II of the bill. We believe this legislation provides critical corporate transparency and strengthens accountability of both U.S. and foreign Internet communication service companies. With other processes under way that will shape the regulatory context of this industry, such as the development of sector-specific human rights due diligence guidance for the European Commission, GOFA should establish a floor rather than a ceiling for the human rights responsibilities of ICT corporations.

Essentially, GOFA requires ICT companies, both U.S. and foreign that operate in Internet-restricting and are required to file an annual report with the SEC – the Securities and Exchange Commission – to disclose their human rights due diligence policies. This disclosure must specify if policies are consistent with applicable provisions of the OECD guidelines for multinational enterprises, including an independent assessment of compliance to the policies in practice. Noncompliance with these requirements requires the company to issue an explanation, and companies must also disclose their policies regarding responses to Internet-restricting country requests to disclose personally identifiable information and communications, and secondly, a provision of notice where the content – when the content of an Internet search engine or Internet content hosting service is removed or blocked by – at the request of an Internet-restricting country.

While we do support fully the disclosure requirements contained in GOFA, we do believe that there's room to improve the legislation. Our suggestions include the following: on reporting requirements, GOFA requires only ICT companies operating in Internet-restricting countries that are required to file with the SEC to disclose their due diligence policies. We believe this requirement should be universal to all public ICT companies regardless of where they operate. On Internet restricting countries: GOFA requires the State Department to conduct country assessments of freedom of expression with respect to electronic information, including government attempts to censor, to block and to monitor expressions and government efforts to prosecute, persecute or punishment individuals for their expressions. The State Department is then required to publish an annual list of Internet-restricting countries that

exhibit a systematic pattern of substantial restrictions on Internet freedom.
We believe that country assessments of freedom of expression and the compiling
of this list of Internet-restricting countries should be an open and consultative process drawing together civil society groups and other sectoral
experts in making these assessments.

Finally, on safe harbor provisions: GOFA's safe harbor provisions specifies that companies certified as members in good standing of either the Global Network Initiative – GNI –
or similar multistakeholder initiatives are not subject to the full disclosure
requirement. However, as GNI is still developing as a multistakeholder initiative, we believe it is premature to specify GNI as a carve-out for due diligence reporting. The provision should therefore be edited to, A, either remove GNI as a preferred multistakeholder initiative or to, B, amend the provision's definition of a multistakeholder initiative. At a minimum, the provision should be edited to strengthen and clarify which MSI's qualify for the safe harbor.

Criteria should include an annual, independent assessment of members, due diligence policies consistent with the OECD MNE guidelines, public disclosure
of independent assessment reports, public disclosure of member policies both regarding responses to Internet-restricting country requests and provisions of
notice when content is removed or blocked at the request of an Internet-restricting country. We thank Shelly for her leadership on this important issue and the commission as a whole. We appreciate this opportunity
to share our perspectives on the responsibilities of ICT companies in human rights; I thank you for that. Water? (Laughter.) For further information, contact us at ICAR, and happy to answer questions or take comments.

Thanks, Shelly.

MS. HAN: Thanks, Amol. I appreciate that. Next we're going to have Susan Morgan; I'll let her get a drink of water first, go ahead – (laughter) –

SUSAN MORGAN: The water was perfectly timed.

MS. HAN: Yeah. Well – and Amol mentioned a number of things specific to GNI
and I don't – I'm not sure if Susan's going to address those specifically in her statement, but I'm sure during the Q-and-A question we'll have a – session
we'll have a time to maybe (sort ?) some of those out. So I'll turn it over now to Susan Morgan, who is the executive director of the Global Network Initiative.

MS. MORGAN: Great. Thanks, Shelly, and I'd like to start by thanking you and
the members of the Helsinki Commission for conducting this briefing, and also

for giving the opportunity to address the work of GNI in protecting and advancing freedom of expression and privacy rights in the ICT sector. So, GNI is a multisector, multistakeholder group of companies, human rights groups, investors in academics, and we came together, really, to chart an ethical path forward for companies when they're facing requests from governments that could impact on the freedom of expression and privacy rights of their users. Over time, we aim to create a corporate responsibility standard for companies in the tech sector.

Over a two-year period, we – taking in all the different stakeholders, we had a period of really designing and working on creating a set of principles and implementation guidelines. They're based on international human rights standards consistent with the U.N. guiding principles, and they really set out a way for companies to operationalize thinking about freedom of expression and privacy rights in their organizations. For example, that's – things like conducting human rights impact assessments for new markets, new products, new services and also looking at some very, very specific considerations for companies when they receive a request from the government to do a particular thing and how they should respond.

I wanted to say a little bit about the accomplishments that we've made so far, starting off with accountability – and corporate accountability is really at the heart of GNI. Earlier in – earlier this year, in 2012, we completed the first independent assessments of our three founding companies: Google, Microsoft and Yahoo. These assessments were looking at whether the companies were putting in place the policies, procedures and processes to be compliant with GNI's principles. We made public some of the findings in our annual report; there are copies of that on the table. Some examples of the findings are things that the companies were already doing. For example, that the companies have processes in place to review requests from governments that their senior-level oversight of that process and that the companies is putting in place training and communications.

There were, of course, some recommendations for other things that the companies could improve on. Examples of that were more direct engagement with stakeholders when conducting human rights impact assessments and documenting processes around human rights around impact assessments and not dating them as kind of legislation changes within particular countries. The next phase of the assessments, which we're currently working on, will look not only at the policies and procedures that the companies have in place, but whether they're

being implemented in practice with regard to specific cases. Secondly, in terms of our accomplishments, the clear intent behind GNI is that the collective voice of our members – so not only companies, but human rights groups, investors and academic, will bring weight to our growing policy engagement.

So, for example, we worked to raise – early on this year we worked to raise awareness of the human rights implications of a request for proposals in Pakistan earlier on in the year to build a new system for Internet filtering and blocking. We've also issued statements on proposed legislation in Vietnam and Russia that could damage the freedom of expression and privacy rights of users of communication services. Third, in terms of accomplishments, we continue to expand our reach internationally with companies and other stakeholders. In the last 12 months, nine new organizations from six countries have joined GNI. This includes the first new company member since the initiative was launched. We've also created a new category for observers – for companies who are giving serious consideration about joining GNI the chance to work with us for a nonrenewable 12-month period. Facebook and affiliates have now become observers.

And then finally, on accomplishments – I think, given the speed at which the issues evolve in this sector, GNI provides a safe space for different stakeholders to come together to learn and develop best practice. We held our first multistakeholder learning event in June in D.C. this year; we launched a GNI-commissioned report which was looking at the challenges facing governments and technology companies as they navigate their way through – way through freedom expression issues, privacy, law enforcement and national security. We're currently working on best practice guidance on human rights impact assessments.

I wanted to finish just with a few thoughts on both challenges and opportunities for the technology sector. Technology's undoubtedly played a role in supporting democratic aspirations around the world, but it's also clearly been used by governments to aid in the surveillance and suppression of rights. While most commonly identified with China's sophisticated censorship architecture or the shutdown of the Internet under Mubarak's regime during the revolution, issues relating to freedom of expression and privacy are not confined to repressive regimes. For example, draft legislation in the U.K. at the moment on communications data while pursuing legitimate law enforcement goals has some worrying aspects to it, which could give repressive regimes justification for their own approach. It's critically important as democratic countries address legitimate concerns that they consider the international precedent that they could be setting.

Companies are facing new threats from governments in many markets, which are taking increasingly complex and diverse forms. GNI was created to help companies address the ethical questions that arise from these issues and to create a network in which companies could work with other stakeholders both to identify best practice and to develop their commitment to freedom of expression and privacy rights.

A few final thoughts: The challenging of – the challenge of addressing the issues of technology and human rights are too complex for companies to go in alone. GNI has shown it is possible for commercial competitors in the ICT sector to work together on issues relating to human rights. The value of this is magnified when bringing in other stakeholders with different and specific expertise. GNI continues to pursue conversations with companies across the ICT sector including telecommunications companies, many of whom have seen an increased focus on their responsibilities in recent years.

And finally, by working together, we think there's an opportunity for rights-respecting companies to both set a global standard for how companies can responsibly manage government requests in matters of freedom of expression and privacy rights, but also collectively to engage with governments to promote the rule of law and the adoption of laws, policies and practices that will promote respect and fulfill the rights to freedom of expression and privacy. Thanks.

MS. HAN: Thanks, Susan. I appreciate that. Next we'll have – finally have Meg Roggensack from the Human Rights First. If you could take the floor.

MEG ROGGENSACK: Thank you, Shelly. I'd like to thank you and the members of the Helsinki Commission, both for conducting this briefing and for your leadership on these issues. It's really a great opportunity for all of us to consider the challenges that we face, and really the role that the Helsinki Commission and the Congress can play in helping to drive awareness and promote changed behavior.

I wanted to just start by asking everybody here, how many of you – raise your hand if you've actually been in a fire drill – raise your hand. So pretty much everybody. Now, keep your hand up if you've actually been in a fire. Has anybody actually been in a fire? I bring this up because why do we do fire drills? We could say, you know, nobody's been in a fire. This is a lot of – you know, takes a lot of time, it's a big disruption in our business day. And

you know, we're not fire safety experts. Why are we – why are we doing this?

Well, we do it because the risk of not doing it is one that we deem unacceptable. And it's indicative also, this drill, of a broader awareness of health and safety issues. In a nonprofit – a little nonprofit, a big law firm or the bureaucracy of the U.S. government – whether big, small, whatever, we all know how to get out of the building in the case of a fire whether we ever encounter a fire or not.

I bring this up because it really is, I think, a crude but applicable example to the challenge we're facing today, which is that you can say at a global level most users of Internet services are never going to face, you know, dire consequences. But for those that do, the consequences of censorship, surveillance or tracking could be, and are, life-threatening. And so, like fire safety, it's unacceptable for companies to wing it. And so the conversation today really is about not only are what the consequences of winging it, but what are the alternatives to winging it and what are the broader implications that we're facing.

Secretary Clinton, about two years ago, gave a landmark speech on Internet freedom, in which she really related the core freedoms of the universal bill to rights in cyberspace and declared the freedom to connect. And she warned of the consequence if we failed to protect this freedom, which would be whether we live on a planet that had one Internet and a common body of knowledge that benefits and unites us all or a fragmented planet in which access to information and opportunities in dependent on where you live and the whims of censors.

So companies in this sector are on the front lines in this battle. And they're getting demands from governments to surveil, censor, limit service or otherwise provide users' information. And the decisions that they make have a wider impact, not only on the sector but on all of us, whether we have an open access to information and a safe way to use the Internet.

We know that the human rights challenges are significant and that they're evolving nearly as rapidly as ICT products and services and that they affect a whole range of companies, not just Internet providers but telecoms companies, credit card providers, manufacturers of mainframes and switching technology. We also know in the past year alone that the governments have taken down both entire services as well as specific content in Egypt, Pakistan, Vietnam, Iran,

Afghanistan, Libya, Indonesia and India.

Iran has launched its own censored and controlled country-specific intranet and China has imposed a warning system to chill Twitter users' speech. Secretary Clinton, recognizing the pivotal role that companies can play, declared that "American companies need to make a principled stand. This needs to become part of our national brand." A key part of that national brand, she noted, is a trust between companies and users so that users know that what they put online won't be used against them.

As we've heard today, the U.N. Framework and Guiding Principles are an important global standard in evaluating what are the responsibilities of both governments and companies. And it's certainly true that states are principally responsible for protecting human rights, but companies also have a responsibility to respect human rights. And the Guiding Principles articulate that as a requirement of due diligence. Simply put, knowing and showing – knowing what the risks are to the global business operations and showing that you have a plan to address those risks and to follow-through and communicate how you are addressing those risks.

The GNI is, at present, the only initiative that affords companies in the ICT sector a platform for addressing human rights due diligence in a comprehensive, credible and transparent way. And I won't repeat what Susan has said about the aspects of the Global Network Initiative that make it unique from a trade association or from other types of initiatives. We helped to launch the GNI because we think that volunteering multistakeholder initiatives can play a very valuable role in helping companies address human rights risks of their global operations. But whether or not these succeed depends in major part on whether they can demonstrate a positive impact on the human rights issue.

So in GNI's case, its effectiveness is going to depend on the extent to which company assertions about what they have done to implement GNI's principles can be verified through independent assessments and then transparent reporting on those assessments. GNI has make important progress, as Susan has noted, and I hope in our question and answer session we'll be able to talk a little bit more about that. But unfortunately, most companies aren't even at the table. They're not even part of the conversation.

We know, for example, that most of these companies have limited, if any, human rights expertise, and most of it is residing at the headquarters level, not at the – in the countries where these issues frequently are playing out. They also don't adequately engage stakeholders, so they have difficulty understanding what exactly is happening in these countries and why and then how to respond to it. And they do, at best, an extremely limited job of reporting on their efforts to address these threats. They don't even consider the possible impacts that their partners, for which they are also responsible.

So these are all major challenges to implementing human rights due diligence. And we would – we would submit that statements about what these companies are doing regarding due diligence can't and shouldn't be taken at face value because there's no way to independently verify whether they have adequate policies in place, whether those policies are being effectively implement, and how, if at all, the company is addressing government demands.

So GOFA is a really exciting development because it has a potential to help ensure wider corporate engagement on this – on this issue. GOFA really zeros in on the challenge of engaging the ICT sector more comprehensively by requiring that companies due diligence policies or explain why they're not doing it. And this requirement should help raise awareness, not only within the sector, about what due diligence is and what companies need to do but also spark what is a really needed debate about best practices. And so we, at Human Rights First, look forward to working with you, Shelly, and others to develop the best possible bill and see that it gets passed.

The threats to Internet freedom are pervasive and proliferating. We know that we can't realize the vision of one Internet without the full engagement of the ICT sector. That vision is vitally important for the millions of people who live under repressive regimes. For them, the Internet is virtual town square. It's essential to them, but also to us, in preserving and promoting democracy and human rights in this century.

MS. HAN: Thanks, Meg. I wanted to – I appreciate all of the testimony that y'all gave today. And I wanted to dive a little bit deeper into the question of – that we ask in the – in the briefing title, which is Online Safety under Repressive Regimes. And what's the responsibility of technology companies? And think about the issue of particularly differing legal regimes and how

companies are having to operate in China or Vietnam or – and some – you know,
some companies are operating in Iran or however.

And if maybe, Amol and Meg, if you could address this more from a philosophical
standpoint or a legal standpoint and, Susan, you could talk about it from how
GNI approaches it. But what really – I mean, our companies should they – is disclosing enough how they work or should they be doing more? And what should
we be asking of companies?

MR. MEHRA: Sure. I'll take the first crack at this. You know, I think, as Meg mentioned, at the international the U.N. Guiding Principles on Business and
Human Rights articulate the companies have a responsibility to respect human rights. What this means essentially is that the standard is that companies should do no harm.

So when they're operating in repressive regimes, I think we would – we would argue that companies should think critically about whether their operations pose significant risks to human rights. And if so, the companies should do no
harm. If that means that the company removes themselves from that situation,
that's one option. Another situation is that the company could exert its leverage to try to change the situation in the country using its market power
to address the potential human rights implications in that way.

But again, Shelly, I'd submit that the real issue here is that companies have a
responsibility to respect human rights. That's agreed upon at the international level. This was universally endorsed at the council. And so now, you know, what that means in practice that companies should do no harm. We believe due diligence is a tool for companies to assess whether or not their
operations pose significant human rights risks, and therefore, you know, we're
very supportive of the measure being included in this bill.

MS. ROGGENSACK: So to just add to that, as Amol said, a first starting point
is to do a risk assessment – which is one element of due diligence as outlined
in the Guiding Principles – and based on that risk assessment to determine whether a company wants to enter that market given those risks and if it's equipped to manage those risks. As Amol said, one consequence of that might be: No, we aren't. We aren't equipped to manage those risks. We can't operate responsibly in this market.

But another alternative might be to think about who in that market one could partner with responsibly and work with that partner to develop both principles
for operating and then a system for monitoring against those benchmarks

going
forward to gauge over time how that's playing out and then report and review on
how that is working and if not, then to make a difficult decision about whether
continuing in that market in on balance harmful or hurtful.

I think, you know, obviously another really important aspect of this, we know
without saying a number of markets that are extremely challenging and that
require often collaborative approaches. As Susan said, companies can't go it
alone. So another strategy, apart from risk assessment, is to work
collaboratively with other companies facing the same challenges and also with
home governments to try to use that collective leverage to fight against market
restrictions more proactively, and of course engaging with stakeholders to do
so. As we've said, GNI's really the only place right now for this sector to
engage and to have a safe space for those conversations and strategies to
address these types of market challenges.

MS. MORGAN: So I just want to add a couple of things to that. I think – so
GNI was really founded on the basis of how can you help companies operate in as
broad a range of markets as possible in a responsible way? And I think, you
know, as both Amol and Meg have said, the importance of human rights impact
assessments and due diligence, both prior to going into markets and I think
also acknowledging that the situation doesn't necessarily stay the same in
markets. You know, I think we've seen lots of examples in many countries
around the world in the last few years of sort of drastically changing
situations in particular markets. So I think that this sort of analysis and
due diligence needs to be an ongoing process, not a kind of you do it once and
that's it, it's done.

Certainly within GNI, I mean, Meg's mentioned a safe space sort of aspect of
GNI. We've started increasingly to come together as a group of participants to
look at particular issues in markets as they're changing and to really develop
a strategy and approach and a collective response to particular issues, and you
see that in some of the public statements that we've made. So I think those
are really the key points that I'd highlight.

MS. HAN: Great. Could you – Susan, I was wondering if you could – you gave
one example of the issue of the Pakistan request for procurement about the
censorship software and your – GNI's membership response to that. I mean, have
you seen, over the course of the life of GNI, some other examples of specific
changes, maybe, perhaps, that companies have made to their business practices,
or seen a change in the market because of what the principles that GNI is

working on?
MS. MORGAN: So I think there's probably two things to this. The first is the policies and practices that the companies are putting in place. And I think, you know, clearly some of the companies that are members of GNI already had some policies and practices in place before they joined GNI. But obviously in GNI's principles and implementation guidelines, we set out very clearly the expectations of the sort of processes and systems that companies will have in place to be compliant with our – with our principles, and I think the outcome of the first independent assessments earlier on this year showed that, you know, the companies were clearly making progress, but that there was – there was some aspects where there was – where there was more to do.
I think on the "is it making any difference in the kind of wider context," sometimes it hard to say that. Sometimes it's the things that didn't happen.
And you can never – you know, you can never quantify that, but I think, you know, certainly we've definitely had feedback that – from a number of sources that the – you know, the variety of policy engagement that we're beginning to do, whether that's public statements, whether it's responses to consultations on legislation in particular countries, whether it's private meetings with ministers in particular countries on particular aspects of legislation, that that's starting to make a difference. But I think, you know, we're kind of at the beginning of that journey.
MS. HAN: And also, I'll keep you in the spotlight for a second. On membership, GNI membership, you've steadily added companies over – and how – what's your sort of long-term projection? Do you see this growing as basically more U.S. companies as participants, or is the idea to have more of a global engagement? And what are you hearing in terms of what the large companies in Europe are doing, particularly the telecom companies?
MS. MORGAN: So the – the sort of aspiration and vision for GNI over time has always been that we would create a global standard of corporate responsibility in the ICT sector. That's very much the aspiration and continues to be the case. As you say, we've had a steady sort of number of organizations joining us, and I think it's important, you know, not only from a company perspective but also the fact that we're attracting investors, human rights groups and academics from quite a few different countries around the world now. From a company perspective, we've had two new member companies join us in the last year. We've also created an observer status. So some of the feedback that we've had from companies was that they were thinking about GNI, they were interested to learn more about us but weren't quite ready to make that leap yet. So we created a category for observer status specifically so that companies could kind of get to know us and see how we worked together and

sort
of see that value before they made the decision.
In terms of the telecommunications companies in Europe, there's a number of companies who have kind of been working together for about a year now called the industry dialogue. They're looking to house their work somewhere in the near future. Earlier on in the summer, they went out to five different organizations that they were considering as a home for their work. GNI is one
of those. And we're continuing to have conversations with them, and obviously
we hope that that will come to a good result.
MS. HAN: Great. Thank you.
I wanted – we mentioned before that in the Global Online Freedom Act, there's a
provision that specifically requires ICT companies to – that are listed in the
U.S. to report to the Securities and Exchange Commission their human rights due
diligence. There's been some discussion about, you know, whether the SEC is the most efficient or most effective place for that reporting to be done. And
you know, as Amol mentioned, it does sort of piggyback on a couple of provisions that were in Dodd-Frank, 1502 and 1504, which are somewhat similar
in that they're provisions that aren't considered the typical investor or accounting-related provisions for SEC reporting. But they're – recently the State Department created a reporting requirement for Burma that is somewhat of
an interesting model for companies to report their human rights due diligence
and the work that they're doing in Burma, given that we are lifting certain sanctions on that country. And – so it's been suggested that perhaps we might
look at that for a model. And I wondered if Meg and Amol would like to comment
on that and – or have any other ideas along those lines.
MS. ROGGENSACK: Sure. Thanks, Shelly. I'll also defer to Amol a bit on Dodd-Frank. But I think that's right. I think usually with the SEC, it may be
more a matter of making the business case. Investors still don't have the information that they need to make the case that reporting is material in an SEC context. I think we know from our reporting from the field that there is a
case to be made, but it's still one that we have to start to elaborate. What
are the dollars-and-cents implications of these policies? The OECD put a number on the cost of the takedown of the Internet by Hosni Mubarak. There are
other statistics out there about the interruptions of service and what that might mean for commerce. We need to get that information in the hands of investors, because I think it would satisfy a materiality threshold that the SEC would require. But to date, I think, you know, more effort needs to be done, and my sense is, that's the major concern. You're certainly right. Dodd-Frank does provide an avenue. We just need to evidence it for this sector. But it's also true that the Burma reporting requirements, which could

stand to be strengthened and improved – and many of us have weighed in on that
– but it does provide another important model so that the State Department might be an alternative place to receive those reports. I know there are staffing issues associated with that, capacities issues associated with that,
but the Burma model does suggest that that could be another additional avenue
for due diligence reporting.
I just wanted to point out that when California enacted the Transparency and Supply Chains Act, it was really an interesting idea, because at that time they
did set a reporting threshold, but it didn't really question the need for companies to look at whether or not they were aware of potential labor abuses
in their supply chain. They accepted that that would probably be more likely
than not, but that it was up to companies to make that determination. So it didn't stop an effort to impose a requirement. And I know that the mere fact
of passage of that law has driven broad awareness among companies that are covered in California, and outreach and capacity building to develop policies.
It's certainly possible for a company to comply with a law by saying publicly,
we don't have a policy. (Chuckles.) But no company wants to be in that position, so all companies are really obliged to think about their supply chains differently, and I submit that a requirement like this could drive a very important and helpful conversation, whether lodged at the SEC or in the State Department, but it is overdue.
MR. MEHRA: I'm going to agree with everything that Meg said. I think what we
– what we believe at ICAR is that nonfinancial disclosure, disclosure about companies impacts on – social impacts, environmental impacts and governance issues, is critically important not only for consumers and citizens but also for investors. We have seen investors come out very strongly on the provisions
that Shelly mentioned, Section 1504 of the Dodd-Frank Act, which pertains to extractive industries transparency, the publish what you pay law, and Section
1502, which pertains to conflict minerals disclosures. Investors said in submissions to the SEC that having information about a company's due diligence
practices pertaining to assessing risk in their supply chains was material information that affects their investment decisions. So as Meg accurately notes, I think what we need to do is make a better case for how nonfinancial disclosure is material to investors, expanding beyond the traditional socially
responsible investors and linking in with a larger community. This is why the
GOFA bill is very important, because it articulates another set of issues that
could materially infect – affect investors. If you think of a technology company that is complicit with human rights abuse occurring abroad and the news
gets out, what tends to – I mean, the public reaction to that poses

significant
costs to that company, not only potential litigation risks and the cost associated with litigation, but also for consumer-facing companies a drop in sort of consumer value of that company. So these things are all important. And a bill like GOFA helps companies build internal systems to make sure that
they're assessing those risks accurately.
I'll quickly mention the Burma reporting requirements, which essentially require that companies who are seeking contracts with Burma submit to the State
Department a set of – answers to a set of questions. Question five in the reporting pertains to the due diligence policies and procedures that the company undertakes. What's interesting about the Burma requirement is that the
State Department will then take in the information and then publicly post it on
a website, so it doesn't have the sanction that a disclosure regime will have
whereby either the SEC or aggrieved investors can bring claims against a company for false filings, but it does have that public reporting component. So again, to answer Shelly's specific question, the SEC and disclosure, because
of the enforcement mechanisms and because of the substantial risks that these
issues pose to investors, is really where we see this disclosure line.
MS. HAN: Great, thanks for that. Also, Amol, I just wanted to follow up on one thing that you had mentioned in your statement regarding the safe harbor provision that's currently in GOFA. And this provision, as was mentioned, there is a safe harbor for companies. They don't need to report to the SEC if
they're a member of – we don't – the law – or the draft law doesn't say exactly
GNI but it just describes GNI-type organizations, and so that if they're participating in that, then they don't need to make the reports to the SEC. And one of the things that you mentioned – and I just wanted to see if we could
flesh it out a little bit more – was the – you were saying to amend the provisions definition of a multistakeholder initiative and then that – it should include that there's an annual independent assessment of members and the
due diligence policy's consistent. Did you have any thoughts on who would actually be making the assessment of those multistakeholder initiatives? Because that's one thing that we've grappled with a little bit, is how we could
instill some responsibility into those parts of the bill, but exactly who might
be the body that could do that is still an open question, in my mind. So I'd
be interested in your ideas.
MR. MEHRA: And Shelly, that's a very good point. We fought this similar battle on 1502, on the conflict minerals disclosure. As you know, the conflict
minerals disclosure had a general due-diligence requirement built into the statute. So what happened at the regulatory phase with the SEC was a ton of comments were brought into the discussion about which model would be the best

model to point to for what the due diligence disclosure should look like. In the end, the OECD, who had a system moving at the same time, had developed a very robust five-step due-diligence process. So I would reluctantly submit that perhaps the agency that's tasked with monitoring the disclosure should, through a notice and comment period, consider the very many multistakeholder initiatives or initiatives in this space in pointing to what standards are sort of the – now the best and most protected standards.

And again, I want to clarify, you know, we're not – we're not criticizing the GNI at all. In fact, we think it's a wonderful initiative, and we're hopeful that it will sort of lead to the sea change that it could, but the initiative is on – it getting its legs, as I think we're all kind of agreeing about. And so we're reluctant to see it introduced into a legislative text without sort of proof of its veracity.

MS. HAN: Great. I'd like to open it up to the floor. So if there's any questions that you have, I think the room is small enough that we don't need a mic, if you could just speak loudly. And if you could identify yourself, that would be great. Do we have any questions from the audience?

Yes, please.

Q: Hi, there. My name is Billy Ohn (ph). And this might be a stupid question because I don't have a background in this, but I had a question about the due no harm principle for corporate responsibility. And isn't there an idea that it might be better for a company, let's say Google for example, to comply with the laws in an (oppressive ?) market while exerting pressure for change, rather than leaving the market and leaving it to local providers that might be more vulnerable to state pressure and/or might be less engaged with the corporate human rights principles that we've been talking about?

MS. ROGGENSACK: So this is a question that Google actually faced – (chuckles) – in China, as you know. And ultimately I thought Google's solution was deft. Instead of being the agent of censorship, it moved its services to Hong Kong and let the Chinese government take responsibility for censoring content coming back into the country. And they've had additional challenges in operating in China that have been well-documented and that have affected those services. But at least in that case they were able to get themselves out of the middle, which is where companies often find themselves, and it's an unhappy place to be.

You're absolutely right that there is always a weighing in terms of what

does
this service provide vis-à-vis the risks to society of being unable to provide
it either in a safe and secure manner or in a consistent and reliable way. And
so every company needs to make that judgment, engage with stakeholders on the
ground to try to get a good sense of that, which can also help them try to
design around or anticipate some of those risks. So if they know that there
will be, for example, potential government surveillance, go in with a safe
platform, an encrypted platform and/or tools for users to – and education for
users as to how to use the platform safely.

Be transparent about government requests and how they're – how the company is
responding, what the policy is about responding to those requests. And
benchmark that over time to decide, on balance, are we better off here or not –
because over time we could end up with a set of services that is very less
ideal than where we started. So every company needs to be mindful of that, and
it's an ongoing process.

As Susan said, the reverse is true, that the market could open. We also do
think that companies obviously have leverage in these markets. And right now,
most of the companies with these services are U.S.-based – not all, but quite a
few. And so there is an element of leverage there that could be applied,
should be applied, can be applied creatively, both directly and through
collaborative efforts like the GNI and in working with home governments. And
we'd like to see companies, frankly, do more of that than they're currently
doing.

MS. MORGAN: Yeah, I was just going to echo that. I think it's – often it will
be the case that it isn't the black-and-white "Are you in the market or out?"
It's how you operate in the market. And I think that's where the kind of – the
due diligence, the engaging with other stakeholders and the trying to apply
leverage is absolutely critical.

MR. MEHRA: You know, I also want to add that when we mention the Guiding
Principles on Business and Human Rights, one of the foundational principle is
the state has a duty to protect human rights. And companies in the U.S. that
are registered here or operating here should be exerting their leverage to the
U.S. government to help engage bilaterally with these – in these situations as
well. So companies shouldn't feel like they have to go it alone. I think what

we're doing is – in the civil society sector is putting as much leverage and power on the – and push on the – on the government as we can to push these issues along. And I think we're seeing companies start to do that as well. It just increases their leverage. But good question; thank you.

MS. HAN: Yeah, I think that you – you've – you thought that you were asking a basic question. And – but it's a fundamental question, not a basic question, because I think that what we've seen, and particularly in the larger repressive markets like China – and we've also seen it to a certain extent in Russia and certainly Iran – is that homegrown companies are taking the place of the Facebooks and the Twitters and the Googles. They don't need them. (Chuckles.) And I think certainly you'd see – you could see, over a timeline in China – you know, if Facebook – I mean, I'm not privy to any of their business plans, but if they wanted to enter the China market, I – I'm sure they'd get a percentage but certainly not what they could have five years ago, when there was no domestic Facebook. But they already have several versions of Facebook operating in China right now from domestic companies.

So I think it's a – it's a really good question, and it's something that all of the companies are grappling with. And I think they see exactly that conundrum, is that if we don't go in, there are certain – now, there are other examples – say, for example, Kazakhstan. There was – Google had posted a blog post about this a year or so ago, where Kazakhstan – the government had asked Google to route all of the server – the search traffic just through the dot-kz servers so that they could control – and you know, for such a small market – (chuckles) – in Kazakhstan, Google was able to say no. (Chuckles.) You know, they can't do that in China. You know, the – so you have to look at the markets. You have to look at the – you know, the situation on the ground, and then who are the competitors? And there's also a Russian version of Facebook that operates, you know, within the bounds of what the Russian government wants it to operate. So it's something that will – I think will continue to be an issue.

MS. ROGGENSACK: One thing I just wanted to add to that – well, two things, really. One is that companies that are operating in risky environments also – you know, if they're part of the GNI, the mantra is apply any request as narrowly as possible. Take a look; don't overcomply – don't do that. Analyze

whether it's backed by some legal process, duly legal process. And where possible, challenge. And those are all really good principles to apply in any market. They're sensible principles. We know across the world that companies tend to overcomply, and that frequently happens where they haven't done a risk analysis, where they don't have good stakeholder intel on the ground. Frequently their own employees don't understand the risks adequately enough to calibrate them. So that's a place where companies can do a better job, in calibrating the risk and in responding as narrowly as possible.

The other thing that I wanted to mention is there are also a whole slew of markets where this is completely up for grabs. Egypt is one good example of that, where there's a tremendous amount of leverage not only that companies can exert but also our government, both our government and the U.K. government. And it really is a situation where the question on the table is are we going to have a government and an architecture for these systems that's open or closed? And we have an open opportunity to influence that through a whole array of policy tools, dialogue, conversation, diplomacy, economic pressures, and we should seize it.

And part of, I think, what I've tried to convey, and the rest of us today, is that that's also – should be part of this conversation. There should be proactive, robust discussions about those issues and what's at stake. And we unfortunately don't see that except in the – in the context of the GNI, where we're very much oriented toward those issues – and through initiatives like the GOFA. So this conversation needs to be a whole lot broader, needs to include a lot more stakeholders. The government is doing what it can, is working with other like-minded governments around the world. But it's still not nearly enough for the urgency of the situation.

MS. HAN: Any other questions from the audience?

MS.: Yes, please.

Q: Hi, I'm B.J. (ph).

MS. HAN: Oh, I'm sorry. OK. I actually –

Q: Oh, I'm so sorry. (Off mic.)

MS. HAN: Yeah, that's all right. I'm sorry; I didn't see your hand raised. Could we go with the woman here? And then we'll go with B.J. (ph). Thank you.
Sorry.

Q: Kathy Mulvey with the Conflict Risk Network. And a specific question about conflict-affected areas, where I think investors do recognize the materiality of the various financial, legal, operational and reputational risks that they face. And the Guiding Principles also have a – you know, acknowledge specifically the particular risks in those areas. Conflict can erupt spontaneously; human rights abuses and crimes against humanity can begin in places like that. And I guess how can the legislation and initiatives like GNI anticipate and help companies to respond? And you know, is disclosure enough in those situations? And what other measures – and I think Meg started to touch on this with some of what she was talking about, but –

MS.: (Off mic.)

MS. ROGGENSACK: So thank you for that question and for the good work that you're doing on this, because CRN is doing some really astounding leadership on this, particularly with telecommunications companies. Our organization has worked on elaborating a concept of enablers, which can help companies that may be selling what might appear to be bread and butter-type equipment into situations where they're actually enabling possibility of mass atrocities or genocide.

And so again, it comes back a little bit to what we've been talking about due diligence, about doing a risk assessment. We talk about this in the context of Egypt as well, where companies may have been dealing with the Mubarak regime for 20, 30 years; thought, OK, you know, we're on autopilot. But a simple risk assessment would tell you, if you're dealing with an autocrat, that's not a good situation to be in. And whether that autocrat is in for five years, 10 or a day, you need to have a plan for when that autocrat's time ends. And similarly, in situations such as the one Kathy is describing, if they are volatile situations, one has to anticipate the possibility of an escalated conflict that could lead to mass atrocities or genocide. Look at the risk factors for that, and have a plan in place to begin to address them which includes the types of stakeholder engagement that CRN and others are promoting.

MS. MORGAN: So I think – just to echo again what Meg was saying, I think the – you know, clearly the sort of due diligence aspects are critically important. I think the other thing that I'd highlight is just the importance of relationships and building relationships so that you can reach out at the right – at the right time. And certainly that's one of the things that I've observed at GNI over the last couple of years, is the relationships between the

different constituencies developing so that, you know, if there are particular policies or particular sensitivities that companies are facing, they might be more likely to reach out and also possibly, you know, have those kind of relationships where they can get to people quickly on the ground, to kind of have the kind of, you know, discussions and dialogue that's necessary.

MR. MEHRA: Yes, I'll just quickly – I mean, I absolutely agree with what Meg and Susan were saying. I think – there's an interesting report that came out last week from the Businesses for Social Responsibility. And I'm not trying to plug them, but the report is called "Applying the Guiding Principles (sic; UN Guiding Principles)" – (chuckles, laughter) – "on Business and Human Rights to the ICT Sector (sic; Industry)."

And what's fascinating, I think, about this report is that it highlights some of the critical challenges in the ICT sector – including, as Meg mentioned earlier, the lack of human rights expertise within these organizations and their sort of – the – since – and their lack of engagement with affected groups on the ground. So I think that these are two possible solutions that feed into the due diligence process, really, is trying to understand better how to identify, to address, to mitigate potential human rights risks and their operations, which are particularly more acute in conflict risk areas.

MS. ROGGENSACK: So I think one thing that this points up – it's something that GNI and the ICAR and, I know, you were doing – is trying to aggregate good sources of information for companies, because I know Patrick would agree that, you know, there's a lot of good stuff out there. But for companies it's really hard – (chuckles ) – to locate it in a timely way. And so I do think that it's incumbent on us who are working in this to try to do a better job of aggregating what we do have and the thinking that we have so that, for companies that are trying to do this, that they don't have to reinvent the wheel and that there are places they can go for reports, expertise and guidance on these issues.

MS. HAN: All right. V.J. (ph), right? Is that your name? (Chuckles, laughter). Yeah, OK.

Q: Yes. (Off mic.) I'm B.J. (ph) from NDI, National Democratic Institute. I had a couple of comments. The first one kind of echoes on the previous question a little bit. It's – so with a lot of these technologies, what I've found is that it's not quite simple in the sense that it – (inaudible) – can

be
used to – (inaudible) – the exact same – (inaudible) – proxy can be used to monitor and surveil as well. So in terms of either an initial risk assessment
or the continuous risk assessment, I'm not really sure how that plays in, because that can be – (inaudible). And also, there are a lot of open source films, which are the exact same thing. So it's not so much about selling product; it's – (inaudible) – services that are being provided. And I don't know if this law would target anything like that at all, because – (inaudible)
– or what have you.

And the second kind of related question I had is what – and this is just something I know from previous discussions. What exactly is going to stop companies from selling products, whether it's a device or what have you, and then it's resold, like, twice or thrice and ends up with the bad guys? And they kind of have their hands clean, at least in terms of finance, because – (inaudible) – just sold – (inaudible) – and what happens from there does not really – (inaudible). I – (inaudible).

MS. HAN: Let me just say something really quick – (inaudible) – I think you've
raised a couple of really good issues. The first one, on how to do an effective risk assessment on, you know, items that possibly could have use for
good and for evil, I'll let the panel talk about. But just to give a quick snapshot for people in the audience, there is Title III of the Global Online Freedom Act, which addresses the export control issue which you've raised. And
that is for all U.S. companies; it's a – it doesn't just impact listed companies, but any U.S. company that's subject to export control laws would be
subject to those laws. And what it's – what it's trying to do is get at the sale of things that can be used for surveillance or monitoring or censorship to
governments in countries that have been listed by the State Department to be Internet-restrictive. So that's the – what Title III basically does in GOFA.

But I – I'm glad you brought that up, because it was one of the things that I
wanted to touch on. We – hopefully we'll be doing a separate session just on
export controls, because you know, it requires a separate session. (Chuckles.)
It's not something that we can get into in great detail today. But the – there was recently an executive order that was promulgated by the Obama administration that specifically looks at the export of certain tools – Internet tools such as personal communication tools to Syria and Iran. And it's – the short-term name of it is the GHRAVITY Executive Order, with the H-G-H-R-A-V-I-T-Y. And I can't remember how that actually spells out, what each of the letters stand for, but it's really interesting to me, because in my
mind – and I haven't found another example, but it's the first time where we're
making the link between human rights – the legitimacy of using human rights

as
a reason to stop things for export controls and on the Internet area; we've done it before in certain implements of torture – things that can't be exported, but this is in the telecommunications area. This is the first time
that the administration is making that link, and so I think it's important for
the legislation, and it's something that we're looking at to see how we can use
the precedent that's been set through the gravity executive order and the legislation. So now I'll turn it over to the panel to comment on any of those
things.

MS. ROGGENSACK: Well, I want to commend Shelly, because Shelly has really been
a driver of a policy conversations – really over almost two years, I think – on
this issue, and it's a significant one. It's difficult because, as Shelly mentioned, we have technology that activists desperately need, but also that,
in the hands of repressive governments, as we see in Syria and Iran and elsewhere, can have, you know, life or death consequences. And so again – you
know, it sounds like a broken record, but companies need to do due diligence and understand who they're dealing with and also know their customer. You talked about the reseller issue. We had examples of two California companies
who sold through resellers; subsequent investigation revealed that this equipment was going into repressive regimes and a minimal level of due diligence would probably have helped them to identify that.

So it's a know your customer type of requirement. Under the guiding principles, companies are required to know who they're dealing with. So asking
questions, doing a little bit of due diligence is hard, because these are systems, and some of the things that are sold are kind of off-the-rack. Hewlett-Packard sells servers, and they sell them all over the world. So for them, the due diligence may be a bit more challenging than for some of the smaller companies sold bespoke parts that were an integral piece of the surveillance architecture.

But the other part of it, really, I think, for us, speaks to where the U.S. government could play a more proactive role. As Shelly mentioned, you know, there are some difficulties with administering the export control system in this way. It isn't really designed for that; it's very challenging to try to
tailor it to get the result you want. That isn't necessarily the best policy
approach, but we have thought that both through State, DRL and through the Commerce and other agencies, there could be a forward-leaning effort with the
key companies in this space to talk about these risks and proactively discuss
plans for addressing them, and thinking about how to help educate the companies, give them tools so they can implement these policies, but also

better identify the risks and experiment. What would be some ways to mitigate these risks should they arise, and so we're encouraged by the work that Shelly and others have done along those lines to promote those kinds of discussions.

MS. MORGAN: So I was just going to say a little bit about the reseller issue. I mean, certainly in GNI's principles and implementation guidelines, we make a distinction between where companies have operational control and where they don't have operational control, but we're quite clear that, for, sort of, partners, suppliers, distributors – you know, member companies in GNI should use, kind of, best efforts to, you know, promote awareness and understanding of the – of the guidelines. I would also point you to one of our new member companies, which is Websense, who provide filtering technology. And if you look at their anti-censorship policy, they do an awful lot of their sales through distributors, and it's worth taking a look at their policy.

MS. HAN: Yeah, I just wanted to reiterate. You know, Mr. Smith, you know, considers the export control piece really one of the most important pieces of the legislation because of the implications of these tools getting into the wrong hands, and so the – you know, we've been – we've had a number of conversations with the Department of Commerce, who has generally the most jurisdiction over these types of items, and – and it's interesting – also, I've talked to people in the U.K., and the U.K. government has made some public statements, and they're actually working, I think within the Wassenaar Arrangement to potentially have all of the members of the Wassenaar Arrangement, you know, control these items without having to have legislation on our part. (Chuckles.)

So the administration could actually do it; they don't need legislation to do it. And so, you know, we're watching that closely because I think that would be a wonderful step if we could get all of these governments, because when you do it on a multilateral basis under the Wassenaar Arrangement, then you've – you know, you've essentially shut down the legitimate trade of those items or at least created a framework so that when companies are selling, there's a framework which in the – which – in which they have to know their customer, and then they also have to follow the steps of where that item ends up. They still are responsible; you know, they do – if that's part of knowing your customer, is knowing, are they going to sell it on, and if they are, under what terms they're going to do it.

So all of those things are covered under export control; it doesn't mean

that
it's easy to do or easy to investigate when things do go wrong, but I think, from the examples that we've seen in the media, most of these items – for example, the – what was it – Blue Coat – the companies do know when – where the
items are. (Laughs.) They know who's operating them, because essentially, in
order to get software updates or to have any sort of support for that – for that item, they usually are communicating back with the original software provider. So, you know, there's challenges, but I think there's ways to address them, and I'm hopeful that either through legislation or through, you
know, multilateral initiatives, that we'll be able to get at this issue, and we're seeing more interest – or we're seeing interest in the – in the EU among
members of parliament – in the EU parliament, and in Germany, the foreign – I
think it was the foreign minister who made statements to that effect in terms
of stopping the sale of these types of items. So I think the – it's growing acknowledgment of the problem.

So – all right. Any other questions from the audience? OK. I wanted to see
if the panelists could just give me, sort of, your crystal ball projections on
– you know, it seems like every six months, something happens or there's some
sort of, either, a new technology that comes along or new ways that things are
being used, and particularly in these countries – what do you see are some of
the – you know, either current or upcoming issues in this area that we should
be focusing on, and then – sort of, somewhat related to that is my question of
how – you know, we know what governments should be doing; governments essentially have the fundamental responsibility to protect the human rights, but what should we as Internet users, you know, be doing and be trying to advocate for with the companies that we're doing business with?

MR. MEHRA: I'll start, because my crystal ball for the ICT sector is – my crystal ball tends to focus on, sort of, global policy on business and human rights work, so I'll tell you what I think about the crystal ball for ICT. I
think this is a fast-moving industry, and industry where the rules are changing, technology is changing at a pace that – I mean, I can barely understand. So I think what we're going to see happen, hopefully, is, companies are going to start to engage more actively with organizations like the GNI and people like – with expertise on this issue, like Meg in HRF and groups like CRN to try to understand better how their, sort of, responsibilities to respect human rights play out in a global economy with technology moving as fast as it does.

And I think, at the same time – as Meg suggested earlier, I think, within the

civil society community and the advocacy groups, we need to be pushing for stronger requirements on these companies. Technology really is our gateway to communication and privacy, and we need to be holding it very – we need to be very vigilant about our – the ways that we police that gateway. So I'd like to suggest that, you know – the work we do at ICAR is looking at policy solutions for this exact issue, hence we endorsed the Global Only Freedom Act, but at the international level, too, I think these examples are becoming more and more the issue de jure in the business and human rights space. So we need to be thinking multilaterally and globally about solutions that can address these to ensure that, sort of, this isn't just a U.S.-centric approach.

MS. MORGAN: So I think I'm going to put my crystal ball on governments and the role of government. (Laughter.) And I think one of the things – it's going to be very important to see, over the coming, sort of, months and years, is for democratic governments that are wrestling with really difficult issues around law enforcement and national security – that, when they're formulating policies and legislative responses, that they do so in a way that creates a, sort of, model that would be, sort of, adopted in a – in a good way in other countries. I think – I think democratic governments are going to need to become much more aware of the international precedent-setting role that they have. So I think that's on the government side.

And then, on the user side, I think the difference – in the – in the two and a half years that I've been at GNI, the difference in, sort of, engagement on these issues in the press is just unbelievable. I think probably the question I faced most frequently when I joined GNI was, why does GNI exist? And nobody asks that question anymore. And, you know, I think events that have happened in the last few years have really started to bring it home to users, and I think, in terms of users, sort of—companies having users' trust and gaining and, sort of, retaining the trust of their users – being actively engaged on freedom of expression and privacy issues is just going to become more important.

MS. ROGGENSACK: So, picking up on what Susan said – I think the U.S. government has done a good job of framing the issue and of reaching out to other like-minded governments, but at least here at home, I think we'd all agree that there's still a lot that could be done by way of policy integration.

As Susan mentioned, there are a number of cross-currents; national

security,
intellectual property – the list goes on – where there's a muddled message, and
I think, to the extent that the freedom to connect Internet freedom – whatever
we call it – could be more mainstreamed into the broader array of trade, aid,
investment, procurement policies, the more likely it is that companies will be
part of this conversation. I don't think this can be driven purely from the
human rights bench over at State. There's got to be a wider constituency, and
kudos to Shelly and to the chairman for providing a legislative vehicle which
can also have, I think, a really powerful impact on driving this conversation
forward and accelerating and focusing company awareness.

I think – as I said earlier, we shouldn't be taking at face value what these
companies say about what they're doing. We should be demanding a greater
degree of transparency around what they're doing. There are only two companies
right now that issue transparency reports: Google and Twitter. And as
important as those are, they are limited – and there are good reasons for that,
but the biggest thing that we really don't know is, what exactly are they doing
with the requests that they're getting from governments? And I'm not asking
about a specific request; I'm even asking just in the aggregate. Is the
picture getting cloudier or clearer? Is the situation getting better or worse,
and where can the rest of us help that and governments help that? There's no
way to really know that unless we can get a better dialogue going.

One of the things that I think is so challenging for those of us that are not
in companies is that we don't have the level of understanding of the business
that they do. So we don't understand the risks that they're facing, and the
only way that we can have an informed dialogue is if we can reach a place of
trust or we can share that information a little more broadly, and that's going
to take time. The GNI has really created a place, but it does – it does take
time. We know that from other multistakeholder initiatives, but that is really
the place that we need to get and as quickly as possible. We started 20 years
ago in this dialogue with the footwear and apparel companies, but we don't have
20 years. We don't maybe even have two years. The space is either going to
close or stay relatively open depending on the decisions that we make in the
next three, six, 12 months.

MR. MEHRA: I'm just going to add one thing that, sort of, is in the crystal

ball. At the European level, the commission has – we all mentioned this – the commission has, sort of, chartered a group called SHIFT in New York and the Institute for Human Rights and Business to put together sector-specific guidance on how companies can evidence their responsibility to respect in the ICT sector. This guidance is going to be released, I think, in the new year, so this is something that we should all be keeping an eye out for too. It could provide companies a valuable tool for how to interpret complex things like due diligence into their specific areas and operations. It also will identify the risks that are particularly relevant for ICT companies. So something that's ongoing as well.

MS. MORGAN: Sorry, I was just going to add quickly to that. So, I sit on the advisory panel for that – for that work, and I think there's going to be a two-month consultation period when the guidelines come out in draft format, so there will be an opportunity to comment before they're finalized.

MS. HAN: Great. I appreciate all of the – all of your input and the participation of the audience today. I think Meg really hit it on the – the nail on the head when she said that we don't have time, and I think that, you know, Mr. Smith is feeling quite urgent about having this legislation passed, but also to have the conversations continue that we need to have because the – I mean, even here in the U.S., we're grappling with questions about, you know, shutting off the Internet in the transit system or, you know, questions about cybersecurity and the nexus with Internet freedom, and as Susan mentioned, these are all questions – what we're doing here will certainly have an impact on what other countries are doing, but I think the fundamental thing that we do know is that, pretty much, once the rights are gone, it's going to be really hard to claw them back, and particularly in countries and repressive regimes where you're fighting an uphill battle to begin with, it's going to be even harder. So we've got a lot of work to do, and we hope that you'll participate in the – in the ongoing dialogue that we have, and thanks for coming today.

(END)