U.S. Senator Maria Cantwell

Senate Committee on Commerce, Science and Transportation

Subcommittee on Consumer Protection, Product Safety and Data Security

"The Need for Transparency in Artificial Intelligence"

September 12, 2023

Sen. Cantwell Opening Statement Remarks

[AUDIO] [VIDEO]

Sen. Cantwell: Thank you, Mr. Chairman and thank you to yourself and to Senator Blackburn at the subcommittee level for holding this important hearing. I think we're demonstrating that just as AI needs to be open and transparent, we're going to have an open and transparent process as we consider legislation in this area.

And I want to thank Senator Blackburn for her comments about privacy because I do think these things go hand in hand, having good, strong privacy protections certainly prevent the kind of abuse and misuse of information that could cause substantial harm to individuals.

And I thank the witnesses for being here today to help us in this discussion.

I recently was informed about a situation in my state that I found quite alarming. A family in Pierce County, Washington, received a phone call. A scammer used AI to spoof the voice of their daughter telling them that she had been in a car accident and that a man was threatening to harm her if they didn't wire $10,000. So, I can't imagine what this deepfake meant to that family or the concerns that they had.

And a recent deepfake image claimed a bombing occurred at the Pentagon and that fake image sparked a dip in the stock market.

DARPA is leading the way on important developments to approach detecting AI-generated media. And I plan to introduce legislation in this area.

I think that AI, as was discussed by two colleagues, has amazing potential. I held an AI Summit in my state and saw some of those amazing technologies already being pushed by Allen Institute for AI and some of their early technologies, certainly helping in things like climate and farming and detecting illegal activities in helping us to move forward in important areas of research.

We know that we have choices here. We know we want to continue to empower consumers and make sure that we're stopping the fraudsters. And we want to make sure that any misuse of AI that we are stopping at whatever we can do to make sure that we are protecting American's privacy.

I hope that today's hearing will give us some ideas about how to drive innovation and maintain U.S. leadership in this very important security-related technology and the issues of global competitiveness, that we talk and discover ideas about deepfakes and potential national security issues, the framework for legislation, protect online privacy, and combat discrimination.

I know that we need to grow education in general and our workforce. And the information age has already put great transformations in place. The jobs of tomorrow are here today, but the skill levels for people to do them are not.

We know that we need to invest more from the CHIPS and Science Act and skilling a workforce for tomorrow. That was before AI. With AI, there is an accelerant on that. And that is why I believe that we need something as grand as the G.I. bill was after World War II in empowering Americans for new opportunities in this area.

I look forward to hearing the comments from our witnesses. And thank you again Mr. Chairman for holding this very important hearing about the potential and challenges, but clearly we need an open and transparent system just as we did for the internet so that innovation can flourish.

Sen. Cantwell Q&A With Witnesses

Witnesses:

- **Victoria Espinel, Chief Executive Officer, BSA | The Software Alliance**
- **Dr. Ramayya Krishnan, Dean of the Heinz College of Information Systems and Public Policy, Carnegie Mellon University**
- **Sam Gregory, Executive Director of WITNESS**
- **Rob Strayer, Executive Vice President for Policy, Information Technology Industry Council**

[AUDIO] [VIDEO]

Sen. Cantwell: Thank you, Chair Hickenlooper. And again, thank you and Senator Blackburn for holding this important hearing. And for all our witnesses participating in this. I'm sure it's been a robust discussion on many fronts.

I wanted to go back to, you know, the particulars of what you all think we should do on the deep fakes side. As we see technology being developed, and DARPA playing a pretty key role as it is today in looking at deep fakes and deep fake information.

What is it you think is the landscape of a federal role in identifying? Some have described a system of a watermark, some have described immediate information similar to what Amber Alerts are, or something of that nature. What do you all see as the key tools for effectiveness in developing a system to respond to deep fakes? And we'll just go right down [line].

Espinel: it's a very important issue, I think there's a lot of great work that is being done. Some of it spearheaded by a BSA member, a company named Adobe, that has been working on the content authenticity initiative.

And I think in terms of giving, I know a lot of that is focused on making sure that consumers have more accurate information that is truly easily accessible, that they could access and use and take into account about the generation of AI content and about whether or not that content has been manipulated or altered in other ways. But I also know that there are witnesses at this table that are devoting a great deal of their life and energy to that thought. So I'm going to see the mic to them.

Dr. Krishnan: Senator, first a broad comment about trust. I think trust is a system level construct, so when you think about humans interacting with machines, machines interacting with machines, one needs to think about what are the ways in which we can enable trusted interactions, trusted transactions, to happen between them.

Deep fakes as an example, I think content labeling, and detection tools to go along with content labeling, is absolutely essential to allow for individuals, so when I'm interacting with a piece of content for me to know that whether it was actually AI produced, whether it's a deep fake, so to have that information.

Equally well beyond the technology piece, you need education for individuals to know how to actually process this information so that they can arrive at the right outcome with regard to this interaction between human and machine. Similarly, you could also have machine to machine exchanges of data where you could have, you know, I produce a piece of video content and I pass it on to another machine. This is where standards are important. This is where C2PA, the standard you heard about, combined with watermarking could actually provide the trust infrastructure to address his deep faith problem.

Gregory: I believe there's a number of steps the federal government can take. The first is to have a strong understanding of the existing harms and impacts and really be able to understand where to prioritize with groups who are impacted.

That includes harms we know already like non-consensual sexual images, but also the growing number of scams. The second area would be to focus on provenance and to come up with a standardized way for people to understand both AI provenance and opt-in human generated provenance. The third would be to focus on detection. Detection is not a silver bullet. It is flawed, but its availability is still limited to the people who need it most on the frontlines of journalism, human rights, and democracy. So continued investment from DARPA and others to really resource and support in diverse circumstances.

I believe there's a space for legislation around some specific areas, such as non-consensual sexual images, AI generated CSAM, and potentially political ads that could be taken. And I

believe it is the role, also, to look ahead and understand that this continuing ease of generation of synthetic media means that we'll get more and more personalized and this will have an impact in spaces like social media and platforms. So we should look ahead to those dimensions and be ready to consider those.

Strayer: I will repeat what's already been said, that two things on the technical side, very much to emphasize the importance of having an open standard for provenance and secondly, on the social dimension, you know, digital literacy is going to be really important for these things to be implemented.

So bringing together stakeholders that include the media platforms, consumers, on the digital literacy side for how these tools will be implemented effectively.

Cantwell: So who do you think should be in charge of this? Anybody? Mr. Gregory, you look like you're going to volunteer.

Gregory: I'm going to volunteer, but I'm probably not in the best place. So I will note that I see good leadership from agencies like the FTC, that have been doing good work to support consumers to date. So supporting existing agencies that are doing good work with the resourcing and the support. In terms of the legislative gaps, I am not well placed to observe where those should come from. In terms of the R&D, I think that it has broad support that ideally also goes outside of DARPA to other research facilities, and facilities more broadly in the US.

Dr. Krishna: In my testimony, I think with regard to the content being produced, I think Congress should require closed source and open source models to actually create this watermarking label and a detection tool to go with this label. This is for images and video. Text is a huge issue as to what it's because you could have deep fakes with regard to text as well. And I think research is needed there. So I think it's a combination of things. But I think Congress should take a leadership role.

Strayer: I'll just say, Congress obviously has a very important role to play. I also think that NIST is a place where over time, we've seen them deal with some very difficult problems, come up with new profiles for addressing very specific challenges and developing standards that are universally accepted through a NIST process, and so I think NIST has a key role to play here, too.

Cantwell: Well, that is why in the original legislation that we did with the NAIAC was to establish, you know, getting everybody together and figure out what we think the U.S. government's role and responsibility should be. And while they haven't finished, you know, all of their findings, they've certainly made a list of the directions and recommendations. And so I think they are a good place to look for on this issue, as well, at least from a discussion perspective.

But today's hearing was about stimulating some input about the issues around that. And what you basically are saying is, there's no failsafe way to do this, it's going to need constant participation both on the side of making sure there's not mistakes. This is one of the reasons why I support getting a privacy bill that establishes a hard line against discriminatory action, because then you could always take that action, again, when somebody's had substantial harm, given by a direction, I think the privacy framework we've already laid out to basically stop that kind of activity and protect people.

We've heard a lot from the Civil Liberties community about this, about what you might see is online redlining, and you worry about something in the machine learning environment just putting that into a system and then it being there for years and years without anybody even understanding that there was a discriminatory tactic against somebody, and all of a sudden all of these people don't have the same kind of thing alone that they wanted. And so this is something we definitely want to have a forceful bright line, In my opinion, against, and say that if these kinds of activities do exist, that we will stop them and that we have a strong law on the books to prevent them from happening.

What do you think on the collaboration level from an international basis as it relates to deep fakes and communication? Anybody given that thought about how that framework should operate?

Strayer: I just want to point out one analogy of the past was there was a lot of challenge with violent extremist content online in roughly the mid, you know, mid 2000s, post 9/11. There was something formed called the Global Internet Forum to Counter Terrorism, and that was really the major platforms but then many other players came together to form practices and procedures for getting this extremist content off the internet. And so, some kind of multi stakeholder group coming together to do this is probably one of the best ways that we can see this addressed expeditiously as the problem will grow very quickly as well.

Cantwell: Didn't Interpol play a big role in the early days of the internet and trying to do a similar thing, trying to police against pornography online and catching, you know, bad actors who are perpetrating content?

Strayer: Absolutely. Yeah.

Cantwell: And so that was where an international organization was working in organizations working with them to try to police, I guess, or create standards or information for people to stop those activities.

Strayer: Yeah, sort of a clearinghouse model. I think that's what they pursued.

Cantwell: And do you think that was successful?

Strayer: They were, I think, a big component of it. I think the United States shouldn't shy away from taking credit for a lot of work that it did bilaterally, through the Department of Justice, to educate foreign partners about the ways that they can address things like pornography, that rise to that level that it's criminal. So I think the United States has been a real leader in ensuring security and safety on the internet.

Cantwell: Thank you. Mr. Gregory?

Gregory: So add that one of the gaps that we see frequently. And we support local journalists who are trying to identify deep fakes as well as local civil society as they don't have access to skills and resources.

So looking at mechanisms to share skills, capacity, fellowship, that would bring that expertise closer to the people who need it. The circumstance we see very frequently right now is people claiming that real content is AI generated, and people being unable to prove it's real. And that is corrosive in many contexts around the world. And a lot of that has to do with the lack of access to skills and resources. So thinking about opportunities for the U.S. government to support that.

Cantwell: And so what would that be because now you're talking about a subject very near and dear to my heart, and that is the erosion of local journalism by the commoditization of advertising. And I would say, the non-fair use of big companies not giving media their fair value for content, you're not really you know, it's not your content to keep the advertising revenue when it's within your browser instead of going to the Seattle Times or some other website. So this is a problem. And we have to fix that as well. But you're saying their job is, you know, truth justice in the American way. And how can they detect that if they can't do the kind of investigations? Is that your point?

Gregory: Yes, that they don't have access to the tools that they need. And so as DARPA and others build tools, making sure they're accessible and relevant to journalism and others, IT skills so that those are available, and that could be facilitated through existing programs that provide skill sharing.

I agree with you there is a larger context where this is but a small symptom of a broader challenge to journalism where AI increases those challenges, as well as provides opportunities for journalists to use it.

Cantwell: Well, we definitely heard that in Seattle at our summit, that that, that we already have a problem as it relates to keeping and saving local journalism and I'm very concerned about it, because we've existed as a country for hundreds of years with this kind of oversight to make sure that the process that we all participate in, works and functions and the issues are brought up. And clearly we're seeing places in the United States where journalism has, you know, ceased to have a credible model that's a financial model. And thus, we've seen the rise of

a lot of very unfortunate issues, including corruption, because there's no one there to cover and watch the day to day.

So, it's a very interesting question. You're posing beyond what we do as a government in detecting deep fakes. How do you bring the oversight to those whose job is to do oversight?

Gregory: And whose job will get even more complicated in the coming years with the growth of AI?

Cantwell: And so, do you think that's about misinformation? Or do you think it's bigger than just misinformation?

Gregory: I believe it's a question of misinformation to some extent. It's a question of the easy capacity to create a volume of information that journalists have to triage and interpret. It is a question of that against the backdrop of lack of resources.

Cantwell: Okay, and so what would you do about that?

Gregory: In the US context, it's very hard to work out how to direct further resources towards local journalism. One option would be to consider, as we look at the way in which content is being ingested into AI models, is there any financial support to journalistic entities as they do that? This is obviously something that's being considered in the social media context in other countries. I don't know whether that would be a viable option to address local journalism's needs.

Cantwell: So how exactly would it work?

Gregory: I don't know the model that would work in our context. We've certainly seen other contexts globally, where governments have looked for ways to finance journalism from social media, but it's not a viable option here in the U.S.

Cantwell: Okay, I like that. The phraseology should be: "Local journalism is financing these websites and their models." That's what's happening here. And we just haven't been able to find the tools to claw that back. But if we have to go and look at this fair use issue, we'll go back and look at it, because we're not going to keep going this direction. And AI is an accelerant. It's an accelerant on everything. The information age is [bringing] challenges and AI will accelerate that. But we've got to harness the things that we care about and make sure that we get them right because we want the innovation, but we also want these particular issues to be resolved. So we certainly in Seattle have had that discussion.

Dr. Krishnan: Can I briefly comment on this? So on the first part with regard to the tools, I do think that the kind of infrastructure for trust that we have built up with information security with the CERT with CISA, for instance, that that kind of capability if you built it for AI, as well, which could be fairly quickly stood up with FFRDCs, that gives us the capacity even across

countries to track deep fakes, even if they don't necessarily adhere to a content standard like C2PA. Because I don't think any individual organization has that capacity. But something like the CERT could have that capacity because it will span dot-mil, dot-com, dot-gov concerns, and this capability and expertise will reside in something like that. That's with regard to your first question, with regard to how do we manage and harmonize standards across countries. With regard to the second point, I think it's spot on with regard to fair use, on the one hand, the capacity to license copyrighted content. And that's on the input side, so if you think of the AI models as taking input data from, say, the Seattle Times, or things of that nature, how do they declare first that they're using this data and then compensating the Seattle Times fairly for the use of that? On the output side, the interesting question is, is it the case that the Seattle Times is getting more traffic from the ChatGPTs and the Googles of the world? Or is it the case that the revenue that should have come to the Seattle Times is really going to ChatGPT or Bard. I mean, the argument has been that because they provide that entry point into content, that they're actually directing traffic that otherwise would not have found you. So I think that requires analysis and research of the traffic with regard to who's going where, and who's directing what to these sites? Because I think that gets at this revenue point.

Cantwell: Well, I'm pretty sure about 25% of the traffic that's generated online that big sites are getting from news organizations are really revenue that belongs to news organizations. Regardless of the commoditization of advertising, it is still revenue that belongs to the newspapers. And so my point about this is that our report that this committee, when we were the authors of a report, we found that local journalism was the trusted news source. This is the point. And that you have many voices, that that's the ecosystem that keeps the trust. I mean, somebody could go awry, but guess what the rest of the ecosystem keeps that trust. So I think the Seattle Times would say it's a very viable, identifiable source of trust, if you were creating information off of their historical database of all Seattle Times ever-published stories, which is a very long time, that's probably some of the most trusted journalistic information you could ever get, because they had to be in that business, right? But anybody who would then take that content, and then [do] who knows what with it is a very, very different equation. I want to go back to the international point for a second, because I do think you mentioned a lot of organizations. I'm not sure everybody grasped, or maybe I didn't grasp everything you were saying about that. Do you think the NAIAC should be working in coordination right now with international organizations to discuss what a framework looks like? Or are you thinking this is more siloed within organizations like national security issues versus consumer issues versus other things?

Dr. Krishnan: So the NAIAC does have a group that Ms. Espinel leads, as a working group. The AI futures working group that I lead with regard to this trust infrastructure point that I was making. We have been focused on that. It does have international implications, but perhaps Ms. Espinel can speak more to it.

Espinel: So I have the honor of chairing the international working group for the for the NAIAC Advisory Committee. There are conversations that we're having internally about ways that NAIAC as a committee could be helpful, either in terms of making recommendations to the

Administration, which is our mandate, or perhaps NAIAC as a committee. Some of them I can't talk about publicly here, although I'd be I'd be happy to have follow up conversations. I can tell you about one, though, that I think goes to what you're talking about, which is, I think we believe that it is very important as governments are thinking about what the right approach is to regulating AI or to trying to address some of the concerns that have been raised by artificial intelligence, to make sure that those conversations are happening, not just with the United States, not just with the United States and the EU, not just inside the G7, the OECD, but to try to have that be a broad-based conversation, including bringing in emerging economies that have not typically been as much a part of some of these discussions, as I think should be the case. And so I think if we are going to end up with solutions that are really effective, for example, on deep fakes, that is going to have to be a global initiative. And I think it will be stronger and more effective if those discussions are happening with a group of countries that represent different perspectives. So emerging economies are going to have slightly different benefits and challenges -- they need to be part of that discussion. Well, I'm kind of probably overly passionate about it. So I feel like I've gone on a bit too long.

Cantwell: No, no, the question I was trying to get at -- this committee passed this legislation, we created the NAIAC, we said: "Here's your responsibilities." We hope you've been thinking about this, because we've given you a few years to do so. And so I was wondering if the current thinking was a divide over the complexity of dealing with national security kinds of deep fakes, and, you know, commercial and citizen issues on deep fakes and whether you had reached some conclusion on the international side of: There's a lot to this and a lot to communicate and coordinate. Because obviously, the World Wide Web is a big open system. So you could say the United States is doing this, but you need others to participate. But consumer issues [are] very different [from] how we deal with national security issues. And so has the organization come to any conclusion on that?

Espinel: I think the short answer is no -- not to be overly legalistic, but there are significant restrictions on what I'm allowed to say in a public forum. And I want to be very careful not to cross any lines. So I can tell you that I think there are conversations happening about national security and consumers. On the point, I feel like, it is fine for me to say on the point that you are talking about, I don't see there being a real challenge, I don't see there being a lack of consensus on national security versus consumer issues and be able to engage internationally on that.

Cantwell: Well, they're just different organizations within our government. And I'm pretty sure they are internationally. So it just makes it challenging.

Espinel: It makes it challenging. I'll just say in my capacity [with] BSA, you have, for example, the UK Government is hosting a global summit in the beginning of November. And I think one of the challenges they face is -- who, if you're going to have a global summit that is intended to address the safety of artificial intelligence, which is what the UK has announced, who are you going to have? Who's going to be part of that summit? And how many issues can they address because there are a myriad of challenges. And as you say, they are often addressed by different

parts of government. Speaking just in the context of the United States, I think having effective coordination across the federal government, I think there's more that could be done there. And I think that would be very, very helpful because you don't want these issues to get siloed. You don't want agencies to be doing things that are duplicative or in conflict.

Dr. Krishnan: And I'll reach out to your office, Senator, about the trust infrastructure point that I made, I'm happy to provide additional information.

Cantwell: Well, we all know that we have lots of international organizations that are working on coordination on lots of internet issues as it is today. I think the question is, has anybody with the NAIAC come up with a framework before we start having these kinds of big discussions. So anyway, we'll get more information. I want to turn it back over to Chair Hickenlooper. Thank you so much for again, holding this very important hearing.