FINISHED FILE

INTERNET GOVERNANCE FORUM USA 2021

Scenarios for 2026: Will everything work everywhere?

JULY 15, 2021

4:00 P.M. - 5:20 P.M. EASTERN

Services Provided By:

Caption First, Inc.

P.O. Box 3066

Monument, CO 80132

1 877 825 5234

+001 719 481 9835

Www.captionfirst.com

***

***

>> MIKE NELSON: Great. I'm Mike Nelson a Senior Fellow in the Technology and International Affairs Program at the -- we tackle a lot of big-hairy problems in technology, policy, from Cloud governance to Internet governance to cybersecurity, and we have a very important initiative, the Partnership for countering influence operations. I've been involved with the Internet Governance Forum and the Internet Governance Forum USA since my days at IBM before either organization even existed, and I have to say it's really been

great to see how this organization has evolved and particularly how IGF USA has become such an important place to go to discuss the future of the Internet and the policies that shape it.

Last year we went virtual for the first time, I thought it worked incredibly well, and this year I think it's working even better. That is because we've been able to recruit an all-star cast from all around the country and that means that we are going to be able to take a lot of different looks at the issues on the table.

I am in many ways glad that this is the last panel because we're going to touch on many of the topics that were dealt with in earlier panels, Internet of Things, security, data protection, digital identity, Internet filtering, content moderation, censorship, these are all tough, tough issues and they're global issues. The problem is that in each case the first knee-jerk reaction of policymakers, both in national capitals and in state capitals is to ban or block problematic apps or websites or technologies, even if there is a lot of collateral damage.

Our job today is to look at what's happening, what national governments and state governments are doing to try to control or shape the Internet, and then talk about alternative approaches that meet their policy goals without necessarily -- without the collateral damage.

So, I'm going to introduce each speaker in turn, starting with Nick Merrill. Nick is going to do the very hard job of giving us an overview of how the different countries are taking action to try to block the net at different layers in the stack, different techniques they might use, and what that looks like when you actually look at how traffic is flowing, where it's flowing, where it's not flowing. Anyway, Nick is the Director of Daylight Lab at UC Berkeley and a very data intensive guy. But today we're not going it show a lot of slides, and he's just going to give us the data blocking, data filtering, Internet control 101 lecture. Over to you, Nick.

>> NICK MERRILL: All right. Thanks for the introduction,

Michael. Let me share some slides with you. I'm assuming everyone can see these. Again, my name is Nick Merrill, I run Daylight Lab at the UC Berkeley Center for Long-term Cybersecurity. Today I'm going to tell you the what and why of Internet fragmentation.

So, before we dive in, the most important thing to understand about the Internet is that it is composed of different technologies that are layered on top of each other in what's often called a stack. You often hear about the Internet stack, and at the bottom of that stack we have the physical connections that, you know, connect the Internet together, undersea cables, terrestrial cables, make the Internet work, and various technologies are built on top of these physical cables all the way up to this kind of legal or human layer.

Now, fragmentation or censorship or blocking or whatever you would like to call it, can happen at any layer of the stack. The most basic or brute way to do this is to simply disconnect or cut the cables. It is a rough tool, but it has 100% success of disconnecting people and at various other layers of the stack there are ways to do some more fine-grained blocking. The very, very top layer, can you go and sue or arrest someone who sees content they're not supposed to see and an obvious or well-publicized example of this is RIAA or MPAA used to go after people that pirated music or movies, and in between these layers you have things like the great firewall and other ways of blocking websites.

The point here is that methods for fragmenting the Internet are diverse. There are many different ways you can technically implement website blocking, and the details are out of scope for this talk.

Now, just because there are diverse ways for blocking content, it doesn't mean we can't make comparisons. What you see here is similarities of different countries and what content is available on the. Countries that block similar content are closer together in this map. You can see here there is one cluster, and I guess I don't have the pointer here, but one cluster which basically represents this global or mostly global Internet. Around that

cluster there are some countries that are flirting with a bit of censorship, Vietnam, Singapore, Bulgaria, Ukraine, they aren't sure how free or let's say open or unregulated their Internet should be. Then you have around the periphery extensive blocking, China's pattern of blocking is somewhat unique, Venezuela is it extremely unique and only basically block things embarrassing to political leadership there, and then we have a cluster on the periphery that's kind of similar to one another, Russia, India, Turkey, Saudi Arabia, Korea, interested in blocking pornography, content to drugs, content related to illegal gambling, and what you see is although the strategies are diverse, there are patterns at the global level as far as what makes different things accessible.

Now that we've covered kind of what fragmentation is and what it looks like, a key question is what drives Internet fragmentation? Another way of asking this question, and the way I like to ask this question is why fragmentation? Of all the things that could happen to the global Internet, why is fragmentation the thing that we see. Here is some background, some necessary background to kind of tee up this answer to the question, my answer to the question.

Number one, there are only three points here. Here is point number one. Point number one is that the Internet both reflects and shapes geopolitics. The Internet that we observe is the reflection of different kind of geopolitical relationships, relationships between states, and also as the Internet takes on its configuration, that Internet goes on to shape geopolitics and there is some great work on this that you can follow on this link in the slides that I'll make accessible after this talk.

Point number two, regional blocks, and that is blocks under the same set of laws and rules use it as the dominant logic by way the world is organized and there is a great book about this that my post-doc advisor, Steve Weber just published called *Block by block* and globalization may be weaning in the popularity and what may emerge instead are the regional blocks.

Point three, currently the U.S. dominates the global Internet

and I've written at length about, this and again there is a link you can follow with a blog post that kind of lays this out and also Milton Mueller has a great book called *Will the Internet Fragment* that covers this in detail as well. These are the three critical points you must understand about the Internet before we can answer about why fragmentation.

So why fragmentation? Well, Internet fragmentation is the observable -- I'm sorry, the observable effect of nations challenging the U.S.' dominance over the Internet. Another way of saying this is Internet fragmentation reflects this global shift away from globalization and towards these quote, unquote, regional blocks, and these are basically two ways of saying the same thing and you can meditate on why or how they are the same thing somewhat later.

But quickly, and before I wrap up, I'll tell you one more thing. We can detect these emerging blocks by measuring Internet fragmentation, and I have this op ed that you can follow, show me who bans Tik Tok and I'll show you the future Allies, and the idea here again is that there is a correlation between the Internet and geopolitics and they reflect and shape one another. Oh, have I frozen here? Oh, dear.

>> MIKE NELSON: It appears you have. It might be good to use the chat to share the URL for your editorial.

>> NICK MERRILL: Sure thing. Please whoever is in charge if you stop my screen sharing because it appears to be frozen.

>> MIKE NELSON: Thank you. Are you wrapping up now?

>> NICK MERRILL: I, unfortunately, have no choice. I will say one more thing that is basically this map that you saw earlier, the cluster, you can imagine that those clusters, and again I'm sorry you can't see the slide, moving around over time and this is basically using these Internet measurements how we detect geopolitical changes forecast to the degree that we can geopolitical changes using Internet measurement. And with that, I will wrap up and my name is Nick Merrill and can you follow me on Substack at NickMerrill@substack.com and thank you Michael for letting me give

this brief introduction.

>> MIKE NELSON: Thank you for raising to the occasion and challenge and that was not easy to do and I think we have now a better sense of how and why the net is being blocked. I've been on lots of panels on the splinternet and what happens when different countries try to impose rules on the global Internet and I know a lot of people on the call have also done that and there's lots of good work being done by organizations like the Internet and Jurisdiction Policy Network, Access Now the Internet to name just three organizations. And what's different with this panel is we're looking at scenarios that don't just explore what is happening, they explore why it's happening, and what might happen in the next five years that would accelerate this trend towards segmentation, splintering of the Internet.

In particular we're going it look at four different things causing nations to take action. In every case that we're going to explore, there is probably three or four different things going on. There is always a little protectionism, and a little bit of national pride. But in each of our four scenarios, each of our four speakers will talk about, there is a key question that countries are trying to answer, and so those questions are, first, how can a country protect itself better from cyberattacks? Second question is how can governments protect their citizens private personal data. The third driver, a question causing nations to try to segment the Internet and impose their own rules within their boundaries is just fear of foreign content and apps. You know, do I want my kids playing with some game from another country? And then the last issue is about cybercrime and terrorism and how is the Internet being used by people who would do my citizens harm. So, these are lingering issues, but those of us involved in politics know that what often happens is that some big incident kind of drives action. 911 gave us the USA Patriot Act and it's possible in the coming years that we'll see something like the colonial pipeline hack that led us to all learn what ransomware was, but something even worse, 10, 20, 30 times worse that could

lead to a flood of legislation, not just in Washington, but in capitals around the word. I'm going to ask that you give us a four-minute speculation of how is it that the Internet could go bad, break apart in the next five years; and most importantly, how can we change the conversation to give people new answers to their questions? (feedback).

Our first topic is cyberattacks, and our first speaker is Melissa Hathaway. She's the President of Hathaway Global Strategies and worked for both the Bush Administration and the Obama Administration in the White House designing a comprehensive national security strategy. (feedback). I'm going to turn it over to her. Not an easy task, but give us your thoughts on where are we going and is fear of cyberattack going to lead to the fragmentation of the net?

>> MELISSA HATHAWAY: Thanks, Mike. I'm really happy to be here with many of my colleagues. So nice to see you again. I wish we were all in person to be honesty with you. Absolutely, cyberattacks pose an increasing risk to our public health and safety, to our critical infrastructures and services, and to the vital national networks. And what's happening is that Russia, China, United States, and many other countries are starting to install government-controlled filters and monitoring of malicious traffic on the key critical infrastructures and national networks. We're seeing data localization being imposed to pronounce government authority over these critical networks. You're seeing the declaration of trusted and untrusted companies and therefore their applications and services that might be brought about. We're seeing challenges with data portability and we're seeing now the emergence of an arms control conversation that has been accelerated by the attacks that we have seen.

I think it's important to put it into a context. I'm just going to go back five years of where I think the inflection point began, and this was the acceleration of governments intervening in the marketplace and starting to declare sovereignty over the infrastructures and data that transits them. And I think that the

seminal year really was 2017. In May of 2017, you had the first globally implemented ransomware conducted by North Korea called Want to Cry, effected rail, health care, telecom, brought down the majority of the UK healthcare system. A month later followed by another one attributed to conduct by Russia of a weaponized software update that actually destroyed key industries around the world in more than 100 countries and caused more than 100 billion dollars of economic impact, and within that you saw key transportation and logistics systems brought offline with one of the most important companies being hit with a shipping company that represented 7% of Denmark's GDP. It took them months to recover and you started to see a national conversation in many countries starting to talk about what needs to be done.

And then in that very same month, you saw an industrial control system operational technologies from Triton malware targeted against Schneider electric industrial control systems and was designed to sabotage and map the networks and conduct remote control over those operational networks, and as you know it brought about a challenge with a chemical facility in Saudi Arabia that could have actually been a natural disaster.

2018 was the year of the data breach of collecting personal identifiable information about the top five breaches being Marriott, Equifax, Cafe Pacific, Facebook, and British Airways and you started to see the monetization of our citizen data and the underground market and profiling for the artificial intelligence algorithms where we're starting to see algorithmic warfare being used to perfect the new algorithms behind the facial recognition technology.

In 2019 it was ad hoc innovation. It was blocking the Internet by authoritarian governments to actually promote their own political stability in 35 countries. You saw DNS hijacking and targeted malware against core infrastructures and you saw the unique use of drones now to shut down aircraft in key airports in New Jersey, London, United Kingdom and Milan Italy. In 2020 it was the year to exploit and exploit the situation of COVID, and you saw

that really 9 rapid uptick of ransomware and distributed denial of service attacks up almost 700% in key markets, and the theft and disruption of vaccine research, and then key things that happened. In the United States you had united health care services brought offline, 250 hospitals in the United States no longer able to service the sick. You had Israel and Iran going back and forth between the port systems and the water supply systems, and then of course we ended 2020 with the largest breach of an ICT industry and undermining the trusted fabric of every enterprise in critical infrastructure with solar winds which we still see today.

2021 brought it home with the beginning of the colonial pipeline knocking off oil and gas in the whole east coast of the United States, and conducted by another ransomware gang. JBS Foods who had significant economic costs and started to think about agriculture safety, food supply safety, when you no longer can move beef or pork into the marketplace. The latest last week is knocking off another IT industry and bringing about liability to the small and medium-businesses and knocking off the food supply of all of Sweden with one supplier. Ireland's health care system brought down for more than a month. Florida water supply nearly poisoned, and you start to see further and further of what's going on.

So, yes, cyberattacks have significantly impacted and countries are taking responsibility to protecting their citizens, for protecting the critical national services, and you're starting to see, and I think, an escalatory aspect between countries that could lead to conflict. So therefore, the reactions that are happening is the governments are installing government-controlled filters and monitoring. You're seeing governments start to take action, extra territorial action against other states to be preventative of trying to take down those malicious activities before they can conduct more harm. We're seeing trusted and untrusted companies being blocked or accelerated in the marketplace, data portability will continue to be challenged as governments start to monetize the data, localize the data, and declare the data sovereign territory

of their government.

Arms control negotiations are on the rise and are going to be on the horizon, and I think the next five years, you're just going to see this accelerate and the tensions between countries going to continue to rise. Thank you. I look forward to the next scenario.

>> MIKE NELSON: Thank you very much. That may be the scariest one. Our next speaker is Harriet Pearson, and I got to know Harriet when I was in the office next to hers at IBM in Washington. She became the first Chief Privacy Officer of IBM, one of the first corporate chief privacy officers anywhere. In the last four or five years, she's been not only continuing her work in data privacy but also become a leader on cybersecurity law and working with companies around the world as senior counsel at Hogan levels. I can't think of a better person to cover the question of how are conflicting privacy rules and requirements for data protection going to lead to fragmentation of the net?

>> HARRIET PEARSON: Thanks, Mike. I hope folks can hear me. It's good to be with you all. I am marking -- I'm not sure I'm celebrating, but at least I'm marking my 25th year of working on these issues, privacy and backing in from privacy and data protection into data security and cybersecurity. And I'll paint a little bit of a picture around both privacy and data protection as well as data localization. I may have a little bit of a good-news story in my view with at least privacy and data protection laws and concerns. You know, on a global scale, I think the battle or the debate over should there be law or not law, and should be the Internet be regulated and you know what we were discussing 25 years ago which is let's rely on self-regulation until there is a need for law in data protection or privacy, and I think that discussion and debate is over now and the question is, well how? It's the how.

Largely around the world, privacy laws, if one looks at Professor Graham Greenleave's compendium and he tracks every year the number of privacy and data protection laws adopted globally and the rise has been pretty impressive over the last 15 years with over 100 or some large number of countries around the world now

have adopted laws that are somewhat similar to what I'll call European-style laws, comprehensive laws that treat information that relates to an identifiable individual, and that's a pretty broad definition, but treat it with I'll call it a cradle to grave set of obligations that apply usually to private sector, corporate company, or non-law enforcement entities, and that rise of those types of laws being adopted is one phenomena that I think will continue. It can't go that fast over the next five years, but it's already been substantially accomplished. And the United States is discussing at the Federal level, of course, such legislation, and although I don't think it will be of the same detail or with the same details. The important thing for the Internet and fragmentation potentially is the data -- there is a data transfer obligation embedded in many of these laws that relates to access or transfer of information that relates to an individual, usually known as personal data, and the question is well how can that be accomplished in a reasonable and not overly burdensome way and is it blocked?

And the short answer from I'll say from a lawyer's perspective, you know, and my colleagues and I have been working through many companies facilitating transfers and global flow, is that, you know, it is becoming -- it has become more burdensome, more compliance focused to transfer information or access information across for commercial purposes, there is no doubt about it, but I think the counter here is that there are mechanisms for doing this. Is it as easy as it was back 25 years ago? No, it is not. It comes with maturation, and the question is well how will we shape it, how will those mechanisms work? I'm sure many of you have heard of and perhaps looked at and worked with this concept of the privacy shield, which was famously invalidated a few years ago by a decision in the New York Court of Justice called Shems 2 and there are mechanisms being put in place to address the concerns offer government, you know, government surveillance and capabilities in other issues that led to the European Court of Justice ruling, and low and behold, Europe recently announced a new and updated set of

what they call standard contractual clauses which are approved for use with some other guidance and some direction on facilitating the legal, legitimate flow of data from Europe to other jurisdictions that. Is an important marker. There will be ways to facilitate transfers.

And with respect to the EU and U.S., discussions are underway at a political level with the new administration here, you know, working on facilitating an updated and renewed or whatever it will be called, privacy shield, which is a handshake between the two jurisdictions to facilitate even further for particularly smaller companies or companies that want to have the ease of that mechanism for going forward.

Trade-based agreements are also places to address personal data flows, and I think there have been some examples of success there. And Europe has increased a number of countries or jurisdictions that it finds quote unquote adequate under its law, for example like Japan and others. And while one can find a lot to discuss and debate around the mechanisms and particulars of these laws, data protection or consumer privacy laws, overall, I would say that the DNA of these laws, about 80 to 85 percent of the requirements are somewhat similar. And so for those operating globally, there is a way or there are practical ways to construct a global-looking view of what is the organization's approach to data privacy, data protection from a commercial perspective, and note that I'm not dealing or touching the government access to information, government surveillance issue because that is complicated, but it was always there. It was always fragmented, and there I think I would kind of go back up to Melissa's point and probably the others will speak to, you know, that this is where discussions need to occur around how we, you know, various blocks and how one does deal with government access to information. Obviously in the United States this has been a fair amount of debate and legal work around it.

>> MIKE NELSON: So, Harriet, before we get into that, that will be another half-hour lecture, so let's not talk about

government access.

>> HARRIET PEARSON: I will not. The bright spot here is -- two bright spots to know about is 80 to 90 percent of steps to comply with these laws are common. These frameworks can be interoperable, and privacy by design and privacy engineering, for those of you that are technologically oriented or process oriented, there is a fair amount of energy in that discipline and that kind of development of discipline and of framework like the NEST privacy framework can enable an international approach to privacy concepts, data protection concepts in data technology which is promising, not easy, but promising and I think will advance over the next few years. Data localization is a harder issue to address, and I think it's thorny because the motivation and drivers are sensitivity of data for governments, they want to facilitate law enforcement access, and there is outright protection, so there are risks associated with local organizations that have to be managed and I'll leave it at that.

>> MIKE NELSON: Thank you very much. That was a very tough task but you did it very well. I think the even tougher task will be our next speaker, Deji Olukotun with Sonos.

>> DEJI BRYCE OLUKOTUN: You got it.

>> MIKE NELSON: Thank you very much. We practiced the other day when we talked. He's sort of a multistakeholder man, with the corporate world now, but used to work at Access Now and before that was the person who launched the Digital Freedom program at Pen America and writes science fiction, so he does a lot of scenarios, knows how to do them, and he gets to do a scenario or three or four on how cultural differences between countries could lead to fragmentation of the Internet. Take it away.

>> DEJI BRYCE OLUKOTUN: Thanks. Thanks, Mike. I'm definitely talking in my personal capacity here and I'm going to shift up the tone a lot. I took a pretty broad interpretation of your mandate. I'm actually going to read you a little tiny flash. This is dolled the blue hot blues. It's the year 2026, there is a hotly contested election in Texas that is going to tip the balance

of the U.S. Senate. Two weeks before the election, the candidate lucy dies of cardiac arrest while on a private weekend retreat. Only her family and inner circle know of the death but the election is so close that if the news were revealed, the opposing candidate will surely win. With so much at stake, the team hastily decides to cover up the death believing her normally secluded lifestyle would prevent journalists from asking too many questions. Just in case the team uses off-the-shelf keep fake technology from Russia to release a 15-second campaign video in which she yells, "hook them horns" on the eve of an important college football game. Watching the words a minute pane video late at night while smoking legal Cannabis a blue hop artist, blue hop is a combination of bluegrass and hip hop, questions the authenticity of the campaign video, and he releases a song on YouTube that goes, Garbazian home range alien, don't rob me, show me the body. The banjo riff is surprisingly catchy but more than that catches fire and goes viral for a few minutes. Until YouTube's AI flags the video for takedown and automatically refers the video to the police for inciting violence against a political official. He spends the following day behind bars before posting bail. The election proceeds as expected and she wins by narrow margin. Vindicated by announcement that Garbazian died and talks to popular host, news leads to protests riots and undermines trust in the political process.

There are two reactions to this scenario from 2026, the first is a negative one. Legislators around the world introduce bills banning deep fakes and mandating digital platforms to take them down. Anyone possessing deep fake technology is subject to civil or criminal penalties including in the medical profession. Worldwide, countries should down the Internet around elections citing concerns about interference and deep fakes, and as a cruel aside, advertisers pull their ads from any videos or content with Blue Hop music.

Positive scenario, stakeholder restore trust in the political process. A well-funded global multistakeholder body on deep fakes involving academia, government, industry, and Civil Society is

formed. A clearinghouse, the clearinghouse quickly labels videos of public concern authentic or not based on deep fake algorithms in near realtime. There is transparency around decisions in both plain English and machine-readable format and there is ESG reporting on how platforms handle deep fakes leading to investor scrutiny of platforms. Human rights principles of free expression and proportionality are used as a lens and Internet shutdowns around elections lead to international sanctions. Cultural changes as well. People build reality networks. These are associations constructed from empirically verified truths with trusted interoperability between these networks. These reality networks are grounded in the offline world and linked to online communities through new methods of authentication. Finally, Blue Hop surges in popularity and hot tweed sweeps the Grammy awards.

>> MIKE NELSON: That was amazing. Thank you very much. We'll have to reconvene in five years to see or, yeah, five years -- I guess it will be five years to see what has happened November of 2026.

Okay, David. Give us this scenario for cyber criminals setting our policy.

>> DAVID BRAY: Well, thank you. It's very hard to follow on the heels of that quite impressive and actually all the speakers performing, but I will try to do my best. I was going to say that I often approach covers like this like jazz. I do Grammy jazz improve and try to build off things that have been said in the chats and as well as what's come before me so maybe I'm doing Blue Hop this time trying to make it move forward. So, on cybercrime, I'd like to put forward a premise, which is that the good news is we succeeded in democratizing Internet technologies. The bad news is we've succeeded in democratizing Internet technology, and so that means that people can now do things that were only possible either by large nation states 20 or 30 years ago or very large corporations and we already heard a little about what's happening in the era of what's possible as we see what deep fakes are, and reality is you don't even need deep fakes to do some of the cybercrimes and biggest

one as we heard from Melissa is ransomware which has gone I believe from four years ago it was 5 billion dollars in estimated total global damage, and 10 billion the following year, to 20.2 billion, and so anybody's guess as to what ransomware damages will be this year but it's not a good trend. What we're seeing is that it's cybercrime, but it So, also seems to be cybercrime, and I won't say as a political tool, but it seems at least sanctions as long as it's not used against your own country in some cases. So, we're seeing that be a bit of an issue as some of you may know, that some of this ransomware if you go ahead and put your keyboard in a certain alphabet, it actually deactivates some of the ransomware and I'm not saying that you go and do that but that's appear interesting finding there.

So, we are facing the challenge that as said earlier by Nick, it could very well be the reason why we're seeing a raise in ransomware aside from the fact that the tools are democratized but we're also seeing decreasing failed nation-states so this is a way to make money as long as you don't do it to yourself and it's a way to sort of import capital from overseas, and so it raises interesting questions in terms of both how do we address it. Is this something that can a small startup ever expect to have a suite of tools that a large company or large government organization might have to defend itself? Could, you know, several industries, you know, whether it be schools or library, do we expect them to spend the money necessary to defend themselves or is this something that we need to actually start thinking about ransomware protection as a utility and so I raise this as something to think about in terms of moving forward.

So, but it's not just ransomware as things that we need to be facing. We're seeing increasing phishing and whaling in terms of impersonations. We say about a year and a half ago what was rumored to be a deep fake audio that impersonated the CEO and requested a transfer of funds; and unfortunately, before anyone thought otherwise, the funds were transferred and then they disappeared.

And this is being aided in some respects by the increasing use of Crypto currencies and Bitcoin being one but not the only one. The good news is it seems behind the scenes that governments developed relationships with some of the Crypto currency platforms after the colonial pipeline attack, there was apparently a stop of the payment before it actually reached the individuals, and so that's a success that probably went behind the scenes and should be celebrated, but it does raise questions like will we see nations, and I mean China already band Bitcoin more for concerns about power usage, but will we see other nations say we don't want to allow Crypto currency not only for power concerns but aiding and abetting ransomware payments. That may not be purely the reasons to say and do that, but at the same time we see the raising Crypto currencies we say nation-states launch them, United States is think being a digital dollar and some countries are implementing it, but it may very well be convenient when you launch your central bank digital currency for your nation to also at the same time ban certain Crypto currencies for those reasons to make the swing back to central bank digital currencies, and that then raises back to Harriet's point which is are we comfortable with the privacy that these currencies collect in private information, banking transactions, what you spent, and what can be done with the data, and even if it's deidentified and as we know even the best attempts of deidentification if you have enough dataset you can get it back to the individual. So, the last thing I want to share is we should be prepared for this get messier and harder. For what Melissa said I'm also on the side I think there is going to be increasing cybercrime because that's where the money is. Why do people rob banks? Because that's where the money is. Why do people go after raw data? Because that's where the money is as well. Until there is a better approach to deal with data, expect the data to be held hostage as a source of data because there is money in it. Another thing is space. They may sound strange but there are other efforts going there. At the Geotech Center we're working with companies thinking about putting in space memory and processing power when we

look back at it will be quite tremendous in terms of capabilities possible. And when you can process things in space, you do have to ask, whose geopolitical jurisdiction is it? Is it the jurisdiction that actually chose to launch the satellites, is it something else, and how do we make sure that we don't end up launching the new silk web in space and all the challenges that may come from that as well? And so it's going to be an interesting feature and the last thing I'll say is that at the Atlantic Council Geotech Center, 2020 was a challenging year as I imagine for all of us not just with the pandemic but we succeeded in bipartisan consensus on what the United States means for tech for good in a bipartisan sense with regards to secure data and communications with regards to trust and digital economy, resilience of supply chains, digital health technologies as well as space, and I'm going to share that link in case you're interested and we do also have a one-page cheat sheet if you want to skip the longer report, then can go to the single chart. There are recommendations and as mentioned, we have bipartisan consensus and Mike McCaul from Texas. And with that I turn it back over to you, Mike, and I hope to have a robust conversation now on how to blend this and move forward together.

>> MIKE NELSON: We have 35 minutes to do that, and I want to thank all of you for being very concise, very provocative, and opening the door to lots of good questions. Let me ask a really quick question of you, David, and then I've got a quick question for Melissa. So, one of the issues on the table is encryption and countries trying to impose severe restrictions on the use of encryption, particularly encrypted communication services because terrorists are using them, criminals are using them.

By the year 2026, how many nations around the world will have effective ways to control encryption, the use of encryption by their citizens?

>> DAVID BRAY: That's a good question. I think there is obviously the concern, and I think whether it is putting something in the middle so the encryption looks like it's working when it's not, or basically just trying to put a ban. I think, you know,

again going back to Nick's diagram, if I was to guess, and again if I had a perfect crystal ball, I would be playing the stock market right now but that said I would probably say we estimate about 20%. And we see this as a technology that's being exported and now that said, while we're being caught up in that debate about how many nation-states are going to effectively make encryption moot on the Internet, let's also just be tracking and I'm not saying 2026 is the year, but we should start thinking about also quantum resistant algorithms because it may very well be that we embrace encryption only to find out, I'm sorry, that type of encryption is no longer useful in that area as well. And so I think it's a dual strategy in which personally I am not a fan of devaluing encryption and I'm all for it. I think, yes, there are risks and you have to find other ways to tackle those issues because what you give up is not worth it, but we also need to be ready for when even if we do embrace encryption, for encryption to become as we know it, moot because of quantum computing.

>> MIKE NELSON: Just to do a plug for last year's IGF USA, there was a very interesting debate over this whole question of encryption. Melissa I'm going to give the easiest question. I've gotten several requests, that people want to know what the name of your charming dog is, and whether we can get a picture so we can put it on the pets of the IGF USA.

>> MELISSA HATHAWAY: Sure. My golden retriever is named Kamis after the wine and the Australian cattle Shepard mix because there are two here, her name is Jazz and I'll work on getting a picture of them in this camera here for you.

>> MIKE NELSON: Thank you for bringing them both to the show.

>> DEJI BRYCE OLUKOTUN: Mike, can I ask a quick question for David. You use the term phishing and whaling, what do you mean?

>> DAVID BRAY: Whale something a specialized term of phishing in which you're going after the CEO.

>> DEJI BRYCE OLUKOTUN: Like the example you gave.

>> DAVID BRAY: Exactly.

>> MIKE NELSON: A couple of questions, first to Steve, we

mentioned how national capitals are trying to close down the Internet and the fact is that things are happening right here in the United States, and state laws are being passed leading certain services not to be available, and then I'm going to turn to a question from Amir on the Q&A, and we'll go from there. Steve, your question.

>> STEVE DELBIANCO: Thanks, Mike. This is a true and ongoing example to show a scenario that's both credible and very destructive to innovation and fits tightly with scenario 2. The state of Illinois enacted the nation's first biometric privacy law in 2008, BIPA, biometric information privacy act and intended to address fingerprint data collector who used the information in an unauthorized way. So, the law says that before you collect any biometric information, you require a written notice to the person and then get their written release, just to collect it and not to use it. Well, that entitles in this law, anyone whose data is collected without a written release to a $5,000 claim for every incident without any showing that they were harmed or any intent to harm them. This has been a real boom to predatory trial lawyers and a real pain for Illinois consumers. The Chicago Law Firm Edelson is legendary for having brought class action law suits on behalf of unnamed and unknown consumers in Illinois who may have used facial recognition to tag faces across their own personal photo albums without written release from family members, friends, and teammates whose photos were in the albums. He won over a billion dollars suing Shutterfly, Apple Photos, Amazon Photos, Facebook, and Google; so today, those services do not allow you, an Illinois customer, to tag your own friends and family photos online.

One more. When Amazon and Nest developed doorbells with cameras on them. People everywhere except Illinois have been able to use it to recognize the faces of family members, daycare providers, housekeepers, schedule visitors and deliverymen and both to inform your Nest camera that someone is there and go a step further to unlatch the day if you connect that. That future is not available in Illinois. So, when the legislator who sponsored that

bill saw the unintended consequences, he tried to amend the law, who do you think spent bills against that, the same law firm whose partners have yachts and opened an office in San Francisco. I close by saying law suit abuse by predatory trial lawyers is a particularly American problem and so our international audience at the global IGF, they just nod their heads in amazement, but now this really is very much our problem and more than just an unlikely scenario. So, I'm interested to hear how you panelists think we can avoid this type of outcome via alternate solutions. Thanks, Mike.

>> MIKE NELSON: Thank you. Okay. Harriet?

>> HARRIET PEARSON: So, two quick points on that. Thank you. I think there are other states that have passed biometric privacy laws but lack a privacy right of action and you don't hear about those, and all eyes are on Illinois from a business risk management perspective, and I agree that I think the private rate of action is a key issue in the context of consumer privacy legislation here in the United States, and that is one of the details, and it's a very important detail that is still to be resolved at the federal level, and I think one answer is to have stronger federal law.

But you won't prevent the states from enacting legislation, but I think having a stronger federal law will help, so that's one point.

The second point is that perhaps undenounced to many of you all, Europe has enacted a equivalent of a class action framework via a new directive that is in the process of being implemented member state by member state that over the next several years will actually start allowing for private right of actions, collective actions as they call them there, and that is going to change the game because that combined with the rights under GDPR, General Data Protection Regulation, will actually introduce the dynamic in Europe never present before. Europe has always been regulatory, and it was always a balance between fairly reasonable or rational regulators or the relationship between a regulator and regulated and the stakeholders, and let's figure out what the right approach

is with some way and now it's a lot larger under the GDPR and this now introduces a different dynamic that actually may have the same effect as the prior speaker's illustration and so that's something to keep in mind. I don't have any great suggestions for managing the environment such that more private rights of actions are not enshrined in legislation but I think they're symptomatic of when something is really broke and people are really angry, that's an environment in which allows that kind of thing to occur and I think we're in an era where lots of people are angry for various reasons, let's say it that way.

>> DAVID BRAY: Quick to build on what Harriet just said. I really liked what she was saying in terms of different states but then also the larger nation-state picture. Had COVID not happened, I was waiting for 2020 to be the year in which GDPR collided head on with China's data rule because China's data rule is basically anyone in China, whether you're an individual or foreign national or foreign company, has to make their data available to the Chinese government, and if you don't it's their equivalent of a felony. That is completely opposite of GDPR, but of course the pandemic happened and it didn't get to get determined, but I think we're going to see in the next two to three years, cases where individual nation-states move on privacy and Internet capabilities or state relatives to nation-states will collide and it will be interesting to see how does arbitration happen on the global stage.

>> MIKE NELSON: Harriet, do you have an article or something.

>> HARRIET PEARSON: I'll post it. I'll post it.

>> MIKE NELSON: Let me turn to a question from Amir who really was asking a question of Melissa, but this is also a question for Harriet. As these countries try to impose new requirements to protect therapies of Cyberspace and do things like Mike Pompeo tried to do with the clean network initiative, are they going to succeed? How do you actually do that? And I guess the more specific question is are countries going to do what China is doing now with these very vigorous and Draconian cybersecurity audits? Or are they going to do what Russia is doing which is trying to build a drawbridge, you

know, sort of a way to pull up -- to pull back the connections and isolate Russia's piece of the Internet?

>> HARRIET PEARSON: I defer to Melissa totally on this.

>> MELISSA HATHAWAY: Yeah, I think it's important to go to the previous panel or panel before that, that there is an intersection right now on the digital economy and the competition policy, industrial policy, technology policy, and it's about trade and economics and positioning national champions for, you know, the marketplace. And so I think I see a concerted national effort from a Chinese perspective of positioning, you know, through whether it's the trade deal or the Belton Road Initiative for the national champions in the build out and really kind of changing the -- changing competition broadly, and I also see it in Europe's digital decade of actually becoming more European-centric and I would argue focused on their own industrial policy and positioning national champions or trying to create national champions in a face that they only have U.S. and China national champions delivering. And then the U.S. really not taking a holistic point of view in my opinion, that we're still very capitalistic, laze-faire marketplace and while the clean network initiative is trying to get to a disruptive alliance play to be against what's going on from a China Belton Road Initiative, I think it's got a lot of work that needs to come together from the quad and Trans-Atlantic and broader western alliance, quasi alliance that's not actually working, I think, well together on research and development, innovation, agenda and how to really pool the dollars together. It's really kind of ad hoc marketplace play without a real long-term vision of how you would marry up industrial policy, technology policy, competition policy, and trade. And so this is a battleground of economics, and it's already been underway for a decade, and we're late to the party. So, I think there is a lot more that needs to be thought through, and we have to become much more strategic.

When I teach the -- when I teach this or I talk about it, I think you need to really start to overlay the game of Risk for those of us that remember those games, and then with the game of

the Settlers of Catan on the supply lines and when you play them together you start to see different sorts of strategic properties and how they have to play together.

>> MIKE NELSON: That is a great analogy, and as somebody whose daughter was a big fan of Catan, I really appreciate bringing in the cooperative piece of the puzzle.

This isn't just an economics battle though. It's also a battle of words, and in the chat, there has been a lot of discussion about sovereignty and this whole idea of data sovereignty and digital sovereignty. That sort of biases the choices. I mean, a lot of people are using that word or that phrase knowing that -- saying sovereignty puts you in a 350-year tradition. And who can be against national sovereignty? So, my challenge for you is there a better way to frame it? Is there a different phrase that we should be using when the Europeans use digital sovereignty or data sovereignty? The Swiss actually talk about digital self-determination, which I like a lot better because it's focused on the self and you being able to determine what you want as opposed to what the government wants. But there is also strategic autonomy which is also another great government word, so how do we counter this? How do we being a knowledge that nations have a role here but they aren't the role or the only player here and subdividing Cyberspace isn't as easy as subdividing the European continent.

>> DAVID BRAY: (Laughing). I'll jump on the hand grenade and I'll be interested in what other people have to say, too. I was saying Michael not necessarily the identify defined by geographical voters, but the idea that these were things done by government is really coming into the forefront as can all of these things be done by government for the future ahead and still be effective. And especially for the Internet and everything like that, we need to think about not just -- not just government but two other players, which is obviously the public, but of course also in that in theory is supposed to be embodied in the will of the government but there are challenges and within the government there are fractured and

fragmented tribes there, and then the tech companies. I think if anything you want to talk about the speed at which these will happen, the speed at which the things will happen will happen more on the tech companies and then the public and government will respond, but if we do not have this be a conversation with all three present, and that's hard, because again we're not used to doing that, and I will say that when we were doing the bipartisan commission report in 2020 which the United States was challenging, we also had tech at the table and we thought we would get bipartisan buy in from two different parties but then we go to tech and they say, wait, wait, wait, and we were like oh. So, the sort of how do you do coordinated action with disparate actors that may have different goals is very messy, and I think that is going to be, if we can figure out how to do so in a way that is expedition will be a way to get through the next decade, otherwise we might demonstrate that autocracies that don't ask for anyone else's input may move faster at least in the short term than those actually trying to do a more pluralistic approach.

>> MIKE NELSON: I'm going it put you on the spot. If you can give an optimistic outcome or point us to another science fiction writer who may have given us a world where we're actually going to have empowered citizens and the state will let us have our space and tools and content and our games.

>> DEJI BRYCE OLUKOTUN: Sure. Putting me on the spot a little bit, but you know this is where the multistakeholder initiative, I know people overweight those, but you know taking it or piggy-backing off what David said, I think there are, if you look at some of the competition backlash and antitrust and competition, again, with my writer's hat on here, I think there is a concern if you're a politician that political power is being subsided or overwhelmed by transnational corporations and it makes sense to be asking that question, especially when you're election can -- whether you get elected to office, which is the scenario that I presented, could be impacted by these platforms. It's natural for that or those questions to arise. I think having participated in different

multistakeholder initiatives, I think that was the challenge as well, which is at least the funding models were dominated by the companies that could pay, that was sort of the revenue base, so the bigger you are the more you pay, and it weights things in a weird way. But I think it also has to do with this transparency of how information is shared and how quickly it's shared. You know, transparency, even the best transparency initiatives, if it you think of this information moving across fiber optic networks at the speed of light, transparency is always going to be slower than that. So how quick can you get? How can you share that information in a way that people feel is helpful? So I think that balance of seeing the innovation happening within the technology sector, academia I think has a huge role to play, and those -- you do see those partnerships with tech companies, and I think it raises lots of interesting questions in terms of sovereignty, but I think sometimes we just have to admit that if you are a politician and you're used to having a certain kind of power and there are now actors who are at the table in a way that has never been seen before in history, that that's going to create a lot of tensions around this and maybe motivating some of these behaviors around national sovereignty. I don't know, but I just don't see that wrestling with pure in terms of like, yeah, a giant platform versus someone elected to office or appointed to office. In terms of the science fiction stories, Star Trek managed it all so it's hard to go where people are individuals and are empowered and the federation, but it's all -- that's a good place to go and there are a million different episodes but there are a lot of others that I believed and at this and imagined different kinds of elected sovereignties where it's based entirely on population and you can select which population you participate in around the globe, so there are different thinkers on this.

>> MIKE NELSON: What's the name of that book?

>> DEJI BRYCE OLUKOTUN: I think it's called *Infomocracy*.

>> MIKE NELSON: Thank you. I was on a call last week where there was a book by frank *Cool War* About 50 years ago and according to David, outlines a world that is very scary, and basically all the

countries in the world are using the most vicious cyberattacks they can and disinformation to just bring down civilization and it's a very scary kind of view, and in the 60s it sounded terribly pessimistic but today sounds like a little like our headlines.

One word that's coming up in the chat is interoperability and whether we can get policies that have interoperability built in. I think someone mentioned the universal -- the Uniform Law Commission and they just yesterday approved a draft privacy law for state legislatures and the U.S. Congress to consider, and what they did is they didn't say that this is what you got to do. They said we will accept your privacy policies if you can show that you are compatible with the following existing codes. And that could include the California law, that could include GDPR, and it's sort of a way to say, here is a bar, here are five different ways to reach it. Is interoperability policy something that we can hope for? We did it very well with the Internet. You can run lots of different technology using the same interoperable standard.

>> DAVID BRAY: (Laughing). So, Mike, I say the first step though is, you know, interoperability on what we mean by good outcomes versus adverse outcome, and I think you're going to find that different nations have differing definitions of that, and that's what makes it hard. And so, while it's easier to do it on the tech side, but even then, we have plenty of examples where interoperability should have happened or as I said, you know, as I read in the chat, standards are like toothbrushes and everybody wants to use one and just not somebody else's. So, you know, I think in this way it gets back to the Nick's earlier comments about possible regional blocks and where we can get at least some coalition of partners to at least agree to something that is a definition of what is good versus adverse outcomes within that block, and then try and grow membership in terms of those shared norms and values, then we can work on interoperability. But that begins with, I mean, we often talk about tech for good and we talk about tech for bad but don't define what we mean by good and bad and even within nations there are still differing definitions.

>> NICK MERRILL: One more thing, the privacy, maybe not super unique to privacy but something unique about privacy is that it's extremely contextual, and privacy means different things to different people at different times, and there is a great paper about this called *Privacy Is an Essentially Contested Concept*. So, you know, I think with privacy and with all of these different kinds of interest areas, blocks only get you so far even if the block agrees on particular values with things like privacy interoperability, and it gets difficult because it's so situated in communities and contexts.

>> MIKE NELSON: Thank you. Going back to interoperability.

>> HARRIET PEARSON: Hair I just need to interject one thing on that. However, I'll say and repeat a point I made earlier just with an emphasis, the 80 to 95 percent of the steps that are common across jurisdictions that if you want an organization that collects and manages and handles personal information to be respectful of privacy, the steps that can be taken, can be embedded, are actually common. Contextual, yes. From an individual's perspective. But the processes and rights and frameworks can be common across, and that's why I think effectively we have -- we're on the verge of getting a somewhat rough consistent framework of law, and then it becomes a question of values. You're never going to drop values unless we go to a global culture or blocks of culture which may happen, but it's more likely to be vertical, vertical as opposed to horizontal based on, you know, geography.

>> MIKE NELSON: Other commends on how we can have five different ways to achieve the same goal and get countries to rise that each of those five ways work? Either in privacy or cybersecurity?

>> HARRIET PEARSON: Too broad a question.

>> MIKE NELSON: Okay.

>> DAVID BRAY: Mike, real quick, you might be able to get interoperability on outcomes if that makes any sense. So, if you don't prescribe the manner but at least get convergence on the outcomes that might be something that you can achieve.

>> MIKE NELSON: Any models, is there any place or any other type of law where other than trying to get a global treaty or some kind of single answer we went a totally different approach and allowed people to sort of performance-oriented goals rather than legal standards imposed on.

>> DEJI BRYCE OLUKOTUN: There was a post recently from the remarks with adversarial interoperability what can happen if you're not expressly allowed to operate within the technology but you're able to reverse engineer and make observations on that without being punished so you don't have the positive proactive support of whoever your interoperating with, so a lot of benefits can arise from that and that was more from a corporate competition perspective, but still somewhat relevant that you don't always need permission to interoperate and there can be benefits from not doing that.

>> MIKE NELSON: That was one of the most passionate moments of the conference, at least for me, it was very profound. I've heard him talk about adversarial interoperability before and it's a terrible mouthful and not a good buzz word, but the concept that we allow the laws, make sure that we allow the -- that the law allows people to try to make things work together. The example he gave was that when Facebook was trying to compete against My Space, the Facebook engineers made this great little subroutine that could scrape all of your data off of My Space and puts it over on to Facebook. Well, if someone tries to do that today, to move their Facebook contacts and their posts from Facebook on to a new site, something like Jimmy Whales Wiki Trust platform, Facebook would sue the hell out of them and they could do it using patents and trademarks.

Okay. Other comments? We have about five minutes left. In the chat I posted a note to block by block, no K, and that's the book by Steve Weber that Nick mentioned, a phenomenal book on this issue of how things are moving and how companies are trying to deal with a global Internet with now five different rule books, and also mentioned that Milton Mueller has been an active participant in the chat and he's also got a very good book from about four years ago,

one of the first people to really try to explain the challenges in a layman's language. I don't see any other questions. I see lots of comments in the chat. Any questions from the panelists for each other?

This is too bad. You were all so agreeable. I mean I'm glad --

>> DAVID BRAY: I'll toss out one. I'll toss out one.

>> MIKE NELSON: Three of you were good news/bad news, so for an optimist I was very happy to hear that. David, what's your question?

>> DAVID BRAY: I guess for the panelists to consider, I mean, we see varying types of Crypto currencies and some mean to be minimal if no data exhaust which is an interesting premise, because on the one hand you want people to have choice and everything like that, but I ask for the panelists to think about, what would be for the U.S. and maybe what would possibly others in Europe be, where will they come when it comes to the digital exhaust that's produced either by Crypto currency or central digital bank, and does the individual have the right to turn it off, is it something where if law enforcement kicks in, they have the right to pull it, these are all interesting and thorny issues that will come to a head in the next two or three years so I just raise that for the panelists.

>> NICK MERRILL: One thing on this is just that I think that the thing interesting to me about that question is how it settles. Through democratic, through deliberations of legislature, or will it be settled maybe something more like I don't want to use the word brute force, but however these Open-Source projects achieve a level of hegemony like how Linux achieved a level of it in back-end systems. What does the process look like, how gets to participate, how is that process amended after the fact to get other stakeholders that weren't present initially? Those are the interesting questions.

>> MIKE NELSON: Okay. We have time for one minute from each of you so I'll going to ask for one more scenario, so between now and 2026, which international organization, not inter-governmental

organization necessarily, but what international organization do you think is going to do the most to get the Internet working together and moving in a cohesive global way? You don't have to say the Internet Governance Forum. I don't think anybody is going to. Is there some activity happening out there, something that's happening that we haven't maybe noticed, that could make a big difference in this whole area?

>> HARRIET PEARSON: Mike, I'm going to say my thanks and answer the question that I want to answer.

>> DAVID BRAY: (Laughing).

>> MIKE NELSON: You learned the way of Washington.

>> HARRIET PEARSON: The way of Washington. I don't know the answer to that, but I think just one question and maybe it's a provocative statement because we are IGF here after all, is and I honestly, I work with a lot of different kinds of businesses and organizations, and I wonder how much of the question here or the challenges that were posed of what's the effect on the Internet? You know, the Internet does not seem to be a central part of posing or answering questions because I think for many, for many individuals, perhaps, the Internet is synonymous with the experience they have engaged with other platforms because most are hobbyists or going off into the, many of you are probably part of investing the Internet, but most do not. So, I think there is a challenge here in terms of framing something as for the Internet. And I wonder what happens over the last five years is, does the concept of the Internet come back in some way and evolve? Or does it reduce and not be part of the lexicon that we're using for problem-solving. That's an interesting and sobering question. I'll leave you for that because I have another commitment.

>> MIKE NELSON: I appreciate you joining us I'm so appreciative. I'll talk about the Cloud of all things.

>> DEJI BRYCE OLUKOTUN: I'll go next, Mike. I don't have a specific organization in mind but I think it will be whatever group of folks, and I'll use that term broadly, that can provide trust at speed. So, I think trust is critically important, but to do it at

speed and to do it at the speed the world is moving today, that's really hard, and related to that is this concept of shared realities, that to the extent that you believe people are splintering in what they believe and don't and it's always happened with fewer public squares that's come up in other conversations but how do the shared realities pool together and lead to action. You know, for me ideally because of my background, all of this would be underpinned by human rights that should apply in these contexts.

>> MIKE NELSON: Nick, what's your answer to this question? Is there a sleeper organization, is there a group, is there a community out there?

>> NICK MERRILL: You know, I think this is an intentionally provocative answer, but I think we can't underestimate the capacity of NATO to enforce certain norms in the name of security in order to prevent, let's say fissions forming between allies where it would be not advantageous from a geopolitical perspective. Whether that will actually happen, whether that can happen, I don't know. But you know it's something that I like to think about sometimes and what it would look like and why that might come to pass and so far, as meaningful in serving stability among those.

>> MIKE NELSON: Melissa, you know something about NATO.

>> MELISSA HATHAWAY: I don't think NATO is the answer because that really just excludes the whole fact of what's going on in China and ASEAN. If you expect that this is about the digital economy and about digital flows of data that is monetized and contributes to our economies, the organization that should embrace it for economic stability should be the G20, and because they have 80% of the resources, they have the majority of the population, they have the flows. And if you think of it as the G2, U.S. and China, as the predominant players right now and then, you know, the other economies that are going to buy or participate, that's to me, you know, while the G20 is not as effective as it could be probably, it is the place where the economics play out. And it's a mutual.

>> MIKE NELSON: And the place where the heads of state are meeting.

>> MELISSA HATHAWAY: And it's neutral, not NATO which is not neutral. You have to pick something that is global and that includes the largest economies and biggest powers that can drive change for the world.

>> MIKE NELSON: Yeah. My colleagues and I are doing some work on digital leadership and how the countries that are doing the right things are the ones where the heads of state actually engage and start banging the heads of the ministers together until they come to consensus or come to their senses. So, David Bray, you have the last chance to answer the big question. Is the Geotech Commission the answer or is there some other place?

>> DAVID BRAY: No. No. No. We're simply one piece in a much larger puzzle. I was actually going to say G20, so I give a plus 1 to Melissa and then offer an alternative future as well. So should the G20 not rise to the occasion, it will be those tech companies that are doing Internet in space that create something completely new.

>> MELISSA HATHAWAY: Yeah.

>> MIKE NELSON: They have connected the world and bias the regulations we've been talking about for 75 minutes. Thank you very much. I want to really say thank you to the people engaged in the chat, the questions that were asked. You had an incredibly hard assignment to take on these issues in just four or five minutes and you did it well. I'm going it go back and listen again to make sure I got everything, at least once. I apologize for the technical problems, but I have a voice for radio and a face for radio, so maybe it was good that you didn't have to see my lips move.

Take care, and I hope you'll hang around for the virtual mixology class and learn how to make cocktails and I hand it over to Melinda and say thank you to her and Dustin for making this all work so well.

>> MELINDA CLEM: Thanks, Mike. I think there is something appropriate about having this sort of voice of God for such a big topic here to close us out today. Thank you so much for moderating.

So, it's hard to believe that after 6.5 months of prep that

we've completed this two-day run. I'm so grateful for everyone who helped make this happen. And for all of you for attending and having such an energetic interaction here with all of our different panelists over the last two days.

I want to thank everyone involved because I think we got some great new voices, which is always something that I'm trying to make sure that we do, is broaden our circle here and get new voices with different opinions. I think we had way more frank discussions than I expected going into this, which is great, especially on if you missed the Access Panel or Privacy Panel and Antitrust Panels in particular, a lot more direct conversation and some pretty strong opinions and ideas put forward.

Cat meowing in the background).

I have a cat that's been awake this whole time. We're going to go, as I mentioned before, we're going to go to Remo in a few minutes to do the cocktail hour and trivia, so definitely get your drinks ready and we'll see you over there, and a big thanks again, you know, to Dustin, Makena, our intern she's fantastic, Annette, Joli, the entire steering committee and especially all of our sponsors to all of their help this year.

>> DUSTIN LOUP: And as you can see, I have my party shirt on so I'll see you over there. It did just start to rain so thankfully I had an umbrella over the computer, so don't rain further on this parade and make sure you make it to see Callahan and I for the reception.

>> MELINDA CLEM: See you in a few. Thanks, guys.