UNITED STATES COMMISSION ON
INTERNATIONAL RELIGIOUS FREEDOM

HEARING ON TECHNOLOGICAL SURVEILLANCE OF RELIGION IN CHINA

Wednesday, July 22, 2020

10:00 a.m.

Virtual Hearing

P A R T I C I P A N T S

COMMISSIONERS PRESENT:

Gayle Manchin, Chair
Tony Perkins, Vice Chair
Anurima Bhargava, Vice Chair
Gary L. Bauer
Johnnie Moore
Nury Turkel

C O N T E N T S

- - -

P R O C E E D I N G S

CHAIR MANCHIN: Good morning and welcome to today's hearing on Technological Surveillance of Religion in China. I first of all would like to thank our distinguished witnesses for joining us to offer their expertise on this topic.

I want to thank our commissioners that are in attendance today for this hearing and certainly for the great planning and coordination by the USCIRF staff of which Jamie Staley is taking the lead today. So thank you all. Together we make a team that is going to have an outstanding enlightening hearing today.

The U.S. Commission on International Religious Freedom, or USCIRF, is an independent, bipartisan U.S. government advisory body created by the 1998 International Religious Freedom Act, or IRFA.

The Commission monitors the universal right to freedom of religion or belief abroad, using international standards to do so, and makes policy recommendations to Congress, the President,

and the Secretary of State.

Today USCIRF exercises its statutory authority under IRFA to convene this hearing. Of course, because of the coronavirus, we are still conducting hearings at USCIRF virtually rather than in person.

I would like to begin by acknowledging the tremendous suffering the people of China have experienced under the Chinese Communist government. USCIRF has been warning about religious freedom violations in China since the Commission was created in 1998, and the situation has only deteriorated since then.

It is now clear to the world that the Chinese government has detained millions of Uyghur and other Muslims in concentration camps, forced them to work in factories, and subjected them to sterilization and other genocidal population control measures.

Authorities have continued to wage a campaign to assimilate the Tibetan people, demolishing historic monastic complexes and

arresting Tibetans for possessing pictures of His Holiness the Dalai Lama.

Throughout the country, Chinese authorities have raided underground house churches, arrested Christians who refuse to join the state-run churches, and banned children younger than 18 years old from even attending services.

Meanwhile, the government has banned the Falun Gong and Church of Almighty God movements and ruthlessly arrested thousands of practitioners.

Today's hearing will examine how the Chinese government's use of advanced surveillance technology threatens the freedom of all religious groups in China. This hearing comes in the context of broader discussions around the world about the potential risks of artificial intelligence, facial recognition technology, DNA collection, and social media.

A recent report by the National Institute of Standards and Technology documented that algorithms regularly misidentified Asian and African faces, leading to concerns about "automated

racism." Social media companies have come under increased scrutiny for allowing the proliferation on their platforms of hate speech against ethnic and religious minorities.

It is not our purpose today to judge the morality of these new and emerging technologies. Indeed, with the proper safeguards and oversight, these tools can be harnessed for the good of society. However, that is not what we are seeing today in China where the Communist Party is deliberately using technology to undermine religious freedom and other fundamental rights.

I will now turn to my colleague Vice Chair Tony Perkins to discuss this in greater detail.

VICE CHAIR PERKINS: Thank you very much, Chair Manchin.

In past Annual Reports, and in a report published last September, USCIRF has closely monitored the impact of China's surveillance state on religious communities.

The Communist Party with help from Chinese companies, like Hikvision and Dahua, uses

artificial intelligence systems that can reportedly combine information from video surveillance, facial and voice recognition, GPS tracking, and other data in order to track certain religious communities.

During the past decade, it has reportedly installed hundreds of thousands of surveillance cameras across the country, particularly in Xinjiang and in Tibet, where facial recognition systems distinguish Uyghurs and Tibetans from members of other ethnic groups.

Now this is the first time a government is known to have intentionally used artificial intelligence for racial profiling. Authorities even installed cameras on the pulpits of churches and other houses of worship allowing the Party to identify and monitor anyone who attends services.

Meanwhile, the Chinese government has deployed an army of censors and online tools, collectively known as the "Great Firewall," to continuously monitor Internet activity and remove anything deemed offensive to the Communist Party.

This includes blogs and social media posts

promoting Uyghur or Tibetan culture. Importantly, this virtual world censorship has real world consequences.

In April, authorities raided a branch of the Early Rain Covenant Church while they were holding Easter services online. In Tibet, authorities have detained people for sharing photos of the Dalai Lama in WeChat messages.

Due to the international nature of 21st century technology and trade, the United States cannot turn a blind eye to these human rights violations.

Indeed, key technological components driving China's surveillance state come from American businesses and researchers, while in some cases U.S. companies have actively cooperated with Chinese authorities to make such surveillance possible.

We know China's surveillance industry depends on imports of advanced processors and sensors from American companies, including Intel and Nvidia. According to credible reports, both

companies have sold critical components to Hikvision, which has lucrative contracts establishing surveillance cameras for the camps, the concentration camps, in Xinjiang.

In addition, Thermo Fisher Scientific, a company based in Massachusetts, has exported DNA testing kits that are designed to distinguish between Han Chinese and Uyghurs and Tibetans. Although the company said it halted sales to government entities in Xinjiang, it continues to sell its products elsewhere in China.

Now Google, Google's planned development of Project Dragonfly would have enabled its search engine to conform to China's Great Firewall censorship standards. The company was forced to shut the project down after Google employees protested the initiative.

These examples should concern all of us. For too long, it has been said that American companies could do business in China without compromising their commitment to fundamental human rights and values. We now know that claim was

false.

The information revolution is one of our country's greatest contributions to human civilization. But we also have a responsibility to ensure that the fruits of American innovation are not distorted into a dystopia.

We look forward to hearing from acting Undersecretary Cordell Hull about how the Department of Commerce has already taken important steps to restrict certain Chinese companies from obtaining sensitive American technology.

Now earlier this month, the Departments of State, Commerce, Treasury and Homeland Security issued an advisory warning. Businesses--warning businesses about the legal and ethical risk of assisting in the development of surveillance tools in Xinjiang.

I look forward to hearing from our other panelists about what the U.S. government should do next to ensure that Americans do not inadvertently contribute to religious freedom violations in China and elsewhere.

I will now turn to my colleague Vice Chair Anurima Bhargava to discuss the impact of China's surveillance state on the rest of the world.

VICE CHAIR BHARGAVA: Thank you very much, Chair Manchin and Vice Chair Perkins.

In addition to the concerns raised by my colleagues, China's abuse of surveillance technology is affecting religious freedom around the world. China both exports its surveillance technology and provides trainings to countries, including countries that USCIRF has recommended for designation as "countries of particular concern" or for designation on our Special Watchlist.

For example, many of China's neighbors in Central Asia have echoed China's narratives about quote-unquote "combatting religious extremism" to justify their own widespread crackdowns on peaceful believers.

Chinese, quote, "Smart City" programs are spreading rapidly across Central Asia and observers consider the potential for authoritarian abuse of this technology to rank among the biggest

challenges facing the region.

In fact, we have already seen a number of incidents modeled after China's use of surveillance technology to repress religious expression in Central Asia.

In August of 2019, police in Uzbekistan's capital city of Tashkent rounded up nearly a hundred men and forced them to shave their beards, claiming this was to ensure the men could be identified by smart cameras as part of the country's nascent "Smart City" project.

The government of Uzbekistan had long opposed the wearing of breads, which it considered a sign of potential religious extremism instead of a peaceful expression of one's religious beliefs.

Reports that Uzbekistan's Ministry of Education planned to introduce surveillance technology into their schools raised concerns about how this technology will be used to harass and discriminate against girls wearing hijabs.

Authorities in Tajikistan and Turkmenistan also are known to forcibly shave men with beards or

to harass women in hijabs. With surveillance technology we expect to be used to target even more of them.

To be clear, China is not the only country to export advanced capabilities to repressive regimes. Other countries, including France, the United Kingdom, and the United States also export location-tracking spyware, high-resolution video surveillance, hacking software, and censorship filtering applications.

China has increasingly become a dominant player in this market and does not allow for free and open debate about government surveillance.

These technologies leave few of us immune from harm. We will hear from witnesses about how hijackers likely affiliated with the Chinese government have attempted to use malware to target iPhone and Android devices belonging to Uyghurs and Tibetans living abroad. If successful, these attacks could steal the user's contact information, text messages, and call history.

I look forward to hearing from our

witnesses about how the United States can work with our allies and partners to develop a coordinated strategy to deal with these challenges and strengthen religious freedom around the world.

Thank you. I will now turn the floor back to Chair Manchin.

CHAIR MANCHIN: Thank you so much, Vice Chair Perkins and Bhargava for your comments, and it's now my pleasure as we introduce our first panel, and I notice that Cordell Hull has already opened his video. We appreciate that.

Cordell Hull serves as the Acting Undersecretary for Industry and Security. Through his leadership of the Department of Commerce's Bureau of Industry and Security, Mr. Hull advances the Department's national security, foreign policy, and economic objectives by ensuring an effective export control and treaty compliance system and promoting continued U.S. strategic technology leadership.

His bio is certainly on our website so I'm not going to read the entire bio but certainly

comes with the expertise.

Thank you so much for being with us, Undersecretary, today, and if you please open your mic and begin your testimony. Thank you.

MR. HULL: Thank you, Chair Manchin, Vice Chair Perkins, and Vice Chair Bhargava, for convening this hearing today.

I have a longer statement that I respectfully request be submitted for the record, but today I'm pleased to discuss the role the Department of Commerce's Bureau of Industry and Security plays in administering export controls to address the concerns with ongoing human rights abuses and religious persecution against Muslim minority groups in the Xinjiang Uyghur Autonomous Region of China.

BIS plays an important role in attempting to prevent these human rights abuses, and our efforts are coordinated with interagency colleagues including the Departments of State, Treasury, and Homeland Security.

Since last October, BIS has added 48

parties to our Entity List for repression of Muslim minorities in Xinjiang. That includes 21 government entities and 27 companies.

Earlier this week, we added a third tranche getting us to the 48 that consisted of 11 companies involved in forced labor in Xinjiang.

Our interagency colleagues have been busy as well. For example, on July 9, the Department of the Treasury added four current or former government officials and the Xinjiang Public Security Bureau to Treasury's List of Specially Designated Nationals and Blocked Persons. These Global Magnitsky designations impose financial sanctions targeting abusers of human rights.

The ruling Chinese Communist Party continues to carry out a campaign of repression in Xinjiang, including against Uyghurs, ethnic Kazakhs, ethnic Kyrgyz, and other members of Muslim minority groups. Since at least April of 2017, the PRC government has detained for indefinite periods more than one million members of Muslim minority groups in internment camps designed to eradicate

the detainees' cultural and religious identities.

Former detainees describe appalling conditions, including extreme overcrowding, sleep and food deprivation, torture, forced labor and, most relevant to today's hearing, forced renunciation of religion, denial of prayer and other religious services.

Survivor and family member accounts conveyed through non-governmental and media organizations indicate that CCP uses discriminatory immigration policies targeting diasporic Uyghurs, Kazakhs, Kyrgyz, and others back to China for internment.

There are also reports that some holders of Kazakhstani citizenship have been detained in Xinjiang while visiting family.

The victims of these abuses all have one thing in common: they are members of a Muslim minority that has for centuries peacefully practiced its faith.

In order to maintain the state of repression, the PRC has established an Orwellian

high-technology surveillance system across Xinjiang. Many of these systems are equipped with artificial intelligence, facial recognition, gait recognition, and infrared technology, and those technologies are used to track movements and monitor behavior.

One of BIS' key roles is to prevent exports to foreign parties of U.S. technologies that facilitate human rights abuses. That includes AI and other surveillance technologies enabling the PRC's abuses in Xinjiang.

BIS' export control components generally break along two lines: one, end-user based; the second item-based.

Regarding user-based controls, we can pinpoint controls on bad actors while focusing broader country-based controls on items of specific national security or foreign policy concern.

Through our Entity List, BIS imposes license requirements generally subject to a policy of denial on both government and commercial entities acting contrary to our national security

and foreign policy interests, including in the context of human rights abuses.

To ensure our controls continue to reflect geopolitical and technological realities, BIS has implemented a comprehensive in-depth review of advanced surveillance tools, including facial recognition systems, machine learning, biometric and artificial intelligence technologies, all for possible inclusion in our controls.

In particular, just last week, BIS issued a Notice of Inquiry seeking comments on potential revisions to our control for those technologies, including voice recognition system and others.

In addition to the request for information, BIS along with our interagency colleagues are continuing to review the activities of those involved for potential inclusion in further Entity List action.

As Vice Chair Perkins noted, we have put the business community on notice as well. Along with our colleagues at State, Homeland Security, and Treasury, earlier this month, we issued the

Xinjiang Supply Chain Business Advisory urging businesses to conduct human rights due diligence and to be aware of the legal and reputational risks of doing business in Xinjiang.

The United States government has been unified and consistent in calling for the PRC and CCP to immediately end the campaign of religious repression and persecution in Xinjiang.

I think Secretary Ross articulated our efforts perfectly when he announced the first tranche of Entity listings with respect to Xinjiang last October, and he said, I quote:

"The U.S. government and Department of Commerce cannot and will not tolerate the brutal suppression of ethnic minorities within China. These actions will ensure that our technologies, fostered in an environment of individual liberty and free enterprise, are not used to repress defenseless minority populations."

Indeed, preventing parties complicit in human rights violations and abuses and China's campaign of religious repression remain the top

priority of this administration.

American technologies are created in an environment of freedom and liberty. The role of BIS is to ensure that our technology is not used to undermine freedom across the globe, and that includes in the context of religious repression.

Thank you once again for the invitation, and I look forward to answering your questions.

CHAIR MANCHIN: Thank you so much, and I'm going to begin by asking a question and then moving to other commissioners.

But you talk about working with certainly other groups, partners, in trying to limit or make aware of what is going on there. Do you see this process working that by groups joining together, U.S. allies and partners, that it is starting to make a dent in this persecution of religious groups?

MR. HULL: Thank you, Chair Manchin.

I think the short answer to your question is yes. We believe it's working. We believe that our 48 Entity Listings have impacted millions of

dollars of items going to these entities.

But, of course, the follow-up point is we could, of course, do more, and the Bureau of Industry and Security along with our interagency colleagues are hard at work, as I said in my opening, continuing to assess whether item-based controls or end-use-based controls will add to our arsenal.

With respect to our allies, I'm not aware of any of our allies--I'm not aware of any government in the world frankly imposing export controls for the persecution in Xinjiang. That said, the European Union, the UK, the Australians and Japanese have all expressed their concern with what's going on in Xinjiang, and certainly we hope that we can continue to engage with them and perhaps convince them to follow our lead.

CHAIR MANCHIN: Thank you.

Vice Chair Perkins, do you have a question?

VICE CHAIR PERKINS: I do. Just one quick question, Mr. Hull.

As you are interacting with American businesses, from your perspective or from your experience, how many of them are unwittingly participants in the supply chain or in this chain versus those that may be actively involved, knowing full well that their products and their technology is being used in the fashion that we've discussed?

MR. HULL: Vice Chair Perkins, that is a difficult question to answer, but within my own personal experience, I'm not aware of any U.S. company fully understanding their products are going to repress religious minorities, and I would certainly hope as an American citizen that that would cause a reaction within the boardroom to say perhaps we don't want to do this.

That said, we here at the Department use all sources, including classified information, to determine just that: what is going where and whether particular controls are appropriate? We also have a mechanism within our regulations that if we find items are being used in a particular way, contrary to our interests, we can send what is

called an "is informed letter," and that essentially says, "Dear Company, you are now informed we believe your products are going for nefarious uses."

That's been an effective tool in a wide range of things, and so that is among the tools in the arsenal we have.

VICE CHAIR PERKINS: All right. Thank you.

That's all I have, Chair Manchin.

CHAIR MANCHIN: Thank you.

Commissioner Bhargava. Vice Chair Bhargava, do you have a question you'd like to ask?

VICE CHAIR BHARGAVA: Sure. Mr. Hull, just building on that, I just wanted to ask if there's any other additional tools, authorities that would be helpful to you given all the tools you already have in terms of being able to send this kind of "is informed letters" and other ways in which you can actually ensure that companies are not engaging in ways that are enhancing the capacity of the Chinese government to violate the

rights of religious minorities?

Is there anything else that we could provide in terms of tools or legal authorities that would be helpful to you in that effort?

MR. HULL: Well, I'll start with the legal authority question first. I mean we're quite fortunate that almost exactly two years ago, Congress gave us for the first time permanent statutory authority to enforce dual-use exports.

So Congress has very widely opened the aperture for us, and again our Entity List, to take one example, the criteria for inclusion on the Entity List is acting contrary to the national security or foreign policy interests of the United States.

That is quite a broad category, and obviously we've used that for 48 entities on this particular topic.

In terms of what folks can give us, and I would say this to the Commission as well as I said this to Congress and others, to the extent you have information that particular entities are involved,

please send it. We're happy to take a look at it. We're happy to use the resources of the U.S. government to drill down and try and get to the bottom of it.

If I could answer your question with a request, that would be it.

VICE CHAIR BHARGAVA: Thank you.

CHAIR MANCHIN: Thank you.

Now we have other commissioners certainly in attendance today. Do any of you have questions that you would like to pose to Cordell Hull?

COMMISSIONER MOORE: I'll defer to Commissioner Bauer, and then I'll go.

COMMISSIONER BAUER: Thank you, Commissioner Moore.

Mr. Undersecretary, very informative testimony, and I would like to thank you and your department and the Department of Commerce for focusing on this issue. I think all too often under presidents of both parties not a lot has been done in the past unfortunately.

I have something of a question somewhat

like what Vice Chair Perkins raised, and I'm concerned that some U.S. companies are following an approach of ignorance is bliss. Right? I mean they don't ask a lot of questions so they don't find out information that might require them to make, from their standpoint, profit standpoint, difficult decisions.

And I guess I would ask something ancillary to the specific thing we're talking about. What about the phenomena in Communist China of people being forced into slave labor in factories there? And there are repeated reports that U.S. companies are, in fact, having some of their products made in those slave labor factories?

Is there a way that Commerce or USCIRF can shame those companies by exposing them to the American people? Because I think the reaction among the public would be, would be quite damaging to more than just those companies' reputation.

MR. HULL: Well, thank you, Commissioner, and I, certainly as I said to Vice Chair Perkins, I struggle to believe that companies would knowingly

engage in this, and then you raise the point of sort of willful disregard.

I think one thing that our Entity Listings have done in this space, particularly with respect to forced labor, they are now on a consolidated screening list, and so companies can't hide their head in the sand, as it were. These companies are out there. They've been published in the Federal Register, and if you're using this, I'm aware also that CBP I believe it was three or four weeks ago seized a shipment of hair, of wigs made from human hair that came out of Xinjiang.

And so I think the government is waking up to this. I think putting the business community on notice through seizures, through Entity Listings, through hearings like this, through reports the Commission and other bodies issue, and the Business Advisory, of course, is something that we did to formally put the business community on notice.

But I think the more we can say it and the louder we can say it, to the extent there are companies that are engaging in willful blindness to

this, it gets harder to do that.

COMMISSIONER BAUER: Thank you.

CHAIR MANCHIN: [Microphone muted.]

COMMISSIONER MOORE: I'll ask my question. I think Chair Manchin is muted.

Secretary Hull, your comments have focused mainly on American companies. That's a large subject of this hearing. However, we're also dealing with a China that is benefitting from the forced transfer of American technology; right?

And so our capacity to affect this problem on this side of the world is limited now, and so I'm wondering, number one, to your knowledge, how much of the technology that's being used for all of this America's not involved in whatsoever; and secondly, are there any tools that the Department of Commerce has in order to either disincentivize the use of Chinese technology or inhibit that if that intellectual property actually originated in the United States?

MR. HULL: I'll defer to some of my other colleagues in the Department on wider authorities,

but within BIS, the U.S. government is part of a number of multilateral fora for restricting certain technologies. There is the Wassenaar Group, which is the conventional dual-use goods; the Australia Group, chem-bio; the Missile Technology Control Regime, missiles; and the Nuclear Suppliers Group for nuclear.

And that is usually between 35 and 45 like-minded countries. So that is an important and a very powerful tool that we're able to capture certain technologies that are being misused, but it's a challenge, and it's a challenge because China has for a number of decades now worked quite hard at indigenizing a number of these technologies, whether through IP theft or forced technology transfers or just indigenizing it on their own.

So that is a challenge, and putting export controls on things that China has itself becomes a challenge, but it is something that we certainly work with our allies through those multilateral fora, most particularly the Wassenaar Arrangement,

to try and stanch that off as best we can.

CHAIR MANCHIN: Thank you.

Commissioner Turkel, do you have a question?

COMMISSIONER TURKEL: First of all, thank you very much, Acting Secretary Hull. I am personally grateful for your leadership, that of Commerce Secretary Ross's leadership, designating that many Chinese entities.

I never thought that the entire police department in the Uyghur region would be added to the Entity List. Traditionally, your department were focusing on national security issues when designating entities, but this is extraordinary--the number, the focus. I commend you and your leadership for doing such a significant unprecedented decision to address the atrocities.

It's very similar to what Commissioner Moore and my colleagues were asking. I am more focused on the global effort. This should not be the only matter for the United States concern. Are there any governmental efforts with our allies that

your department and what this administration has been undertaking that you can publicly comment?

This has to be--I often use this metaphor. The boat is too small to tackle this giant adversary, if I may, which is very similar to East German Stasi with AI-powered technology and surveillance to suppress their own population.

So can you comment on that if you could, if any governmental efforts--we need to work with allies, especially the Five Eye countries to address this.

MR. HULL: And thank you. Thank you, Commissioner, for the kind words, and I would imagine, I don't think the Xinjiang police expected to be on the Entity List, as well, but let me try and deal with it this way. Obviously talking about bilateral discussions it's a delicate topic and one which I most often defer to my colleagues at the State Department, but what I can say, we have raised this with allies. We have both in conversations and I think our actions speak quite loudly on this front.

But it is something much like all of our export controls, export control policy, we have frequent, frequent interaction with like-minded countries.

You mentioned the Five Eyes. They're, of course, a great example of that. But we have a number of others too, and it's just convincing them we should be in this together, and you're absolutely right. As much as I wish it were, expert controls aren't the panacea to solve all these problems. They are a powerful tool. They are in many ways effective, but it certainly needs the help of our allies to help us along to make sure that we can stanch this off.

I know Vice Chair Bhargava mentioned being exported to other countries, and that's an area where we need our allies to stand with us.

CHAIR MANCHIN: Are there more questions? I also know we want to get to our second panel, so Acting Undersecretary Hull, thank you again for giving your time, for sharing this space with us today, and perhaps there may be a follow-up

question.

But I would now ask that our second panel go ahead and open their videos, and I will make some brief introductions about them, and then they can go on to speak.

MR. HULL: Thank you, chair.

CHAIR MANCHIN: So first of all, Amy Lehr is the Director of the Human Rights Initiative at the Center for Strategic and International Studies. The HRI was launched in June 2014 and is the only program of its kind in the Washington think tank community. So from this unique position, HRI brings together key actors, catalyzing creative, game-changing solutions to the globe's most pressing human rights challenges through a cross-sectoral and multidisciplinary approach, and certainly there is more to her bio, but you have that in front of you.

Our second witness, Chris Meserole, is a fellow in Foreign Policy at the Brookings Institution and the deputy director of the Brookings Artificial Intelligence and Emerging

Technology Initiative. He is also an adjunct professor at Georgetown University.

Also with us today is Sheena Chestnut Greitens. She's an Associate Professor at the Lyndon B. Johnson School of Public Affairs at the University of Texas at Austin, and a faculty affiliate at the Clements and Strauss Centers.

Her work focuses on East Asia, American national security, and authoritarian politics and foreign policy.

Thank you, Sheena.

And last, but certainly not least, Lobsang Gyatso Sither is the Digital Security Program Director at the Tibet Action Institute. He is a Tibetan born in exile dedicated to increasing cyber security among Tibetans inside Tibet and in the diaspora.

Working with the Tibet Action Institute since 2011, he has helped to develop community-specific technologies and educational content and deploys them via training and public awareness campaigns at the grassroots level.

We welcome each of you here today, and, Amy, I will just turn it over to you now to activate your speaker and share your information with us.

MS. LEHR: Thank you, Chairwoman Manchin, Vice Chairman Perkins, Vice Chairman Bhargava, and honorable commissioners. Thank you for the opportunity to speak to you today.

I'll discuss the challenge that new technologies pose and potential measures to reduce the risks that U.S. technology companies and investors are involved in misuse of emerging technologies overseas.

Emerging technologies are often dual-use. They can be used for good or for ill. Machine learning can help find new cures for severe illnesses, but it can also be used to analyze thousands of images instantaneously to enhance real-time surveillance, including over ethnic and religious minorities.

In China, as you know, these technologies have been used to target such minorities, and we

see efforts in other countries to similarly target political opponents, activists and minority groups.

Indeed, there's a massive global marketplace for new surveillance technology that is deeply opaque, highly lucrative, and frequented by governments with poor human rights records.

This creates particular challenges for both regulators and the companies developing these products. Our thinking must evolve to meet this new challenge.

We need to avoid a race to the bottom. In the long term, a social license to use such technologies will depend on public trust. The U.S. should ensure it's the leading producer of trusted new technology that people are happy to have on their smartphones, for example.

Fortunately, companies do actually have guidance as to how to ensure their technology incorporates human rights standards. They just have to use it.

The UN Guiding Principles on Business and Human Rights, the first global guidance for

companies regarding their human rights responsibilities, were issued almost a decade ago.

They lay out a common-sense management system framework called "human rights due diligence" that businesses can follow to understand and address their human rights impacts.

The UN Guiding Principles have been voluntarily adopted by hundreds of the world's leading companies. I spent a decade helping companies implement these standards. They're understood in the technology sector to mean that companies should integrate human rights concerns into product development--sometimes called "human rights by design."

At various points during product development, they should consider the human rights implications of what they're designing and make sure their design decisions help minimize potential misuse of the product.

They also have a responsibility to conduct research on their customers and the risk of misuse and to not sell the technology if they have reason

to believe it will be used to abuse human rights.

In the U.S., such human rights due diligence is not mandatory although several of our largest technology companies have in place teams and structures to carry it out. The challenge of course is all the smaller companies that don't follow these practices.

Also, it's very hard for companies to pass up customers, especially if their sales are unlikely to become known and lead to reputational damage.

Purely voluntary measures can help companies become more aware of risks and manage them better, but they're unlikely to fully address problems of U.S. company involvement in abusive surveillance overseas.

Recognizing these limitations, the EU has announced an aggressive timeline to pass a law making human rights due diligence mandatory for a wide range of sectors, and a number of large companies have supported this measure.

U.S. technology companies are not the only

actor that may be assisting surveillance of religious minorities. U.S. investors are also a concern. An area that deserves more examination is whether U.S. investors--public and private--are investing in Chinese technology companies involved in severe human rights abuses.

Several large U.S. pension funds were invested in Hikvision when it was put on the Entities List last year. We have no way to know the extent to which U.S. venture capital is being invested in companies known to be deeply involved in the large-scale surveillance of religious minorities.

Indeed, to my knowledge, there is no U.S. body charged with such oversight of outgoing venture capital. Investors, like other companies, have a responsibility to respect human rights. However, this isn't well-known or embedded in the venture capital world in particular.

If a mandatory human rights due diligence requirement for technology and investment companies isn't feasible, disclosure requirements or other

regulatory measures could assist in helping understanding what technology is being transferred and whether U.S. investment is flowing to foreign emerging technology companies that are implicated in abuses.

Last, we need strong global standards for responsible deployment of emerging technology. Right now we're in a rules-free free-for-all. In February, I conducted a research trip to Southeast Asia to understand how facial recognition was being used. We found it was being deployed widely by both governments and the private sector, but with almost no public information on its uses and virtually no legal framework to protect people from abuses of their privacy, assembly or expression.

I'm pleased the U.S. recently joined the Global Partnership on AI and has supported the OECD's efforts on responsible AI. We need to move those forward urgently and then ensure they're translated into national law around the world.

Very briefly, my recommendations include: encourage technology companies to adopt the UN

Guiding Principles on Business and Human Rights; report publicly on their implementation; continue the use of export controls; support efforts to establish mandatory human rights due diligence for U.S. companies and for relevant research institutions; explore mechanisms so that investment of venture capital and sensitive technologies is public or known to a regulator; and, last, support efforts to create global human rights and ethics standards for the development and deployment of emerging technologies.

Thank you.

CHAIR MANCHIN: Questions for--I'm sorry--I thought I had unmuted it. But I think we'll allow our panelists to speak and then come back for questions to each or all of you. But thank you so much, Amy.

Chris.

DR. MESEROLE: Chairwoman Manchin, Vice Chair Perkins, and Vice Chair Bhargava, and honorable commissioners, thank you for the opportunity to speak this morning.

The rise in digital authoritarianism and corresponding decline in human rights, including the right to worship freely, are two of the most pressing issues facing the world today. And nowhere do those two issues enjoy greater urgency than in modern China, where the Xi regime and Chinese Communist Party, or CCP, have relied on digital technology to carry out human rights abuses and curtail religious freedom with unprecedented efficiency and scale.

Before turning to the Xi regime and religion, I should first lay out what I mean by digital authoritarianism. As with all political regimes, authoritarian leaders are obsessed with their survival. Digital authoritarianism refers to the use of digital censorship and surveillance technologies to identify and track dissidents, consolidate regime power and better ensure regime survival.

No authoritarian state has leveraged digital technologies more successfully than modern China. For religious groups targeted by the CCP,

the result has been as devastating as it is tragic.

As with authoritarians elsewhere, the CCP has long been able to repress public forms of religious organizations, religious practices, religious identities, and religious beliefs, especially in urban areas. But private forms of religiosity, including those practiced within one's home, have proven more difficult to monitor and repress.

Digital technologies have changed that. As low-cost processors, sensors and cameras have proliferated, the extent of religious life that the CCP can surveil has expanded dramatically.

Consider the following: first, religious organizations. Not only has video and audio surveillance of public mosques, churches and temples exploded, but digital technology has also enabled greater surveillance of underground religious organizations and networks.

In Xinjiang, for instance, smartphone location data, vehicle location data, checkpoint logs, facial recognition technology and video feeds

from buses, streets and drones can be used to identify when individuals in the same religious network are co-located and meeting together covertly.

Second, religious identities. Surveillance states have long used markers of religious identity such as headwear and jewelry to track and surveil religious minorities.

But digital technologies make such surveillance possible on a larger scale. By feeding machine learning algorithms large numbers of images of religious minorities, Chinese companies have developed software that alerts authorities when it classifies someone in a police video feed as a Uyghur, Muslim or Tibetan Buddhist.

These are being used regularly not just in Xinjiang and Tibet, but even in coastal China.

Third, religious practices. Historically religious practices have proven difficult to monitor without excessive amounts of manpower, yet as with religious identity network video feeds have made it possible to observe religious practices in

a far wider range of contexts, including inside private residences.

These systems make it easier to flag prohibited extremist practices, even when they are performed out of public view.

Fourth, religious belief. Monitoring religious belief has always been difficult for authoritarian regimes because it requires access to an individual's private thoughts, writings, and speech. The smartphone has rendered private writing and speech far more accessible to state surveillance. Not only are Chinese authorities able to monitor messages on WeChat and other applications, but they can also require individuals to install logging software that tracks all video, audio and text stored on the phone or accessed online.

Chinese officials have already used these techniques to detain individuals merely for texting verses of the Quran.

What makes these new forms of religious surveillance so alarming is that they are being

coupled with longstanding forms of mass repression such as detention camps and forced labor.

In Xinjiang, for instance, the Integrated Joint Operations Platform now plays an integral role in tracking the movements, activities and communications of Uyghur Muslims and is the centerpiece for the CCP's surveillance apparatus there. In part, as a result of the IJOP and related systems, an estimated ten percent of China's Uyghur Muslims have been interned in the region's detention camps, where they have been subjected to rape, forced sterilization and abortion and even mental incapacitation.

The United States should seek primarily to counter the CCP digital repression of religion out of concern for the local communities that have suffered so grievously.

But given the scale and severity of that repression, the United States should also seek to deter similar human rights abuses both within China and around the world in the future.

In addition to taking the steps China has

already taken--or the United States has already taken, the U.S. should also consider the following:

First, pressure Muslim allies. If the world has remained silent on Xinjiang, that is at least partly because Saudi Arabia, Turkey, Indonesia, and other major Muslim majority countries have yet to speak out vocally, forcefully and consistently about the plight of Muslims there.

Second, appoint international independent monitors. The CCP has acknowledged the existence of camps in Xinjiang but insists that they are being used solely for educational purposes.

International communities should pressure the CCP into allowing international independent monitors into the region to investigate the camps directly, as well as the use of technology to support those camps.

Third, the United States should also impose targeted export controls. And I'd be happy to speak more about this. But China has struggled to become a world leader in advanced semiconductor manufacturing equipment. The United States should

work with its allies to block the sale of photolithography machines in particular.

Fourth, the United States should also work to develop international standards as was discussed earlier.

For the United States and other democracies to effectively counter digital authoritarianism, it's not enough to critique the irresponsible and unethical use of AI by regimes like the CCP. The United States and its allies must also develop, articulate, and adhere to alternative standards and models for the responsible use of AI and emerging technologies, including especially for use in our own counterterrorism and counter-extremism efforts.

The last note I'll say is the United States can and must push back against the technological surveillance of religion by the CCP, not only to religious minorities within China but all those who want a future with greater religious freedom rather than less.

Thank you.

CHAIR MANCHIN: Thank you, Chris.

And now we'll move to Professor Greitens.

DR. GREITENS: Good morning. Chairwoman Manchin, Vice Chairs Perkins and Bhargava, distinguished commissioners, panelists and guests, thank you for the invitation to speak today about technological surveillance of religion in China.

In recent years, China has accelerated construction of high-tech surveillance state. As you heard today, that system has been used to monitor and suppress the freedoms of millions of Chinese citizens, most notably in Xinjiang, where over a million Turkic Muslims and other ethnic and religious minorities have been detained.

U.S. government officials have described this as the largest mass incarceration of a minority group today, and an increasing number of scholars who are experts on the region characterize it as an attempt to overwrite and eliminate Uyghur culture and religious practice.

Other religious organizations both in China and among diaspora populations have also been

subject to increased surveillance and pressure.

It is important to understand the CCP's strategic objectives in constructing this system. A key term used by China's leaders when they discuss these topics is "fangkong," which translates to "prevention and control."

While Xi's predecessors preferred a doctrine known as "stability maintenance," the current leadership has embraced a much more aggressively preventive version of social control, and Xi Jinping has spent much of the last few years overhauling the domestic security apparatus, its organizations, its personnel, its laws, et cetera, in order to pursue this vision.

Technology plays a central role in accomplishing this mission. Millions of cameras recognize faces and license plates while fingerprint scanners, wifi sniffers, electricity usage monitors installed in homes, and phone apps transmit information on citizens' location, activities, their speech, and more.

But beyond data collection, technology

provides another capacity that is critical to turning technology into coercive power: the capacity to integrate different sources of information. Surveillance platforms combine incoming data, like of the type I described momentarily, a moment ago, with existing information on citizens, their workplaces, their family members, their educational and employment background, biometric and medical data, their previous access or dependence on welfare benefits, and involvement in petitioning or protesting.

Authorities then use that integrated information to assess citizens' risk profiles and decide the best approach to prevent them from engaging in unrest or in dissident behavior.

Although the system is not as omniscient as is sometimes portrayed, it is a high priority for China's leaders and continued improvement and advancement of the system is likely.

Excuse me while I get my papers set. In a recent piece in Foreign Affairs, Julian Gewirtz and I argue that the coronavirus in Wuhan in late 2019

has accelerated the expansion and intensity of China's surveillance state, especially as it relates to public health, and that measures originally intended as crisis coping mechanisms now look to become permanent.

Some of the most serious challenges for religious freedom, however, arise not from the CCP's recent attempts to securitize public health but from the medicalization of policing. Official rhetoric consistently describes dissidence as a political virus or a tumor.

That analogy has significant political implications. The logic of "immunizations" suggests to the CCP apparatus that regime security depends on targeting and "treating" citizens before they show symptoms of politically problematic behavior. That's the logic that underpins the forced reeducation of massive numbers of innocent citizens in Xinjiang and elsewhere.

Moreover, although the regime frames detention as being done with the curative intent of a doctor, it is the CCP, not citizens, that decides

who's at risk of infection and what treatment they shall receive.

The regime's beliefs and interest therefore supersede the beliefs and rights of any individuals.

Official rhetoric has recently extended the virus analogy to Hong Kong, to justify passage of the new National Security Law. This Commission should take seriously the risks that Beijing will approach Hong Kong and even its broader foreign policy with the same prevention and control doctrine that has been applied internally.

China's surveillance technology is, in fact, already a global issue, and I refer you to the two figures that are in the testimony that was submitted through the written record.

Surveillance technology is subject to very few global regulations. Where international standards exist, they have been written largely by Chinese technology companies. My recent research, which was published with the Brookings Institution, shows that China has exported surveillance

technology platforms to over 80 countries worldwide already, particularly those that are strategically important to China and those where violent crime creates an unmet demand for public safety solutions.

As the pandemic has continued, the CCP has also begun to actively promote its surveillance technology as a public health solution, generating risks that COVID-19 will accelerate global reliance on Chinese surveillance technology.

You've already heard today about a number of important policies that could address the development and use of technological surveillance inside China and in the U.S.-China relationship.

I'm happy to discuss those, but let me add one other recommendation that I see as central to the struggle for religious freedom and civil liberty worldwide.

The United States urgently needs a comprehensive strategy to address the risks and threats from the worldwide proliferation of surveillance technology to ensure a future that is

compatible with American values and American interests.

COVID-19 only heightens the existing urgency of this task. Fortunately, we don't need to reinvent the wheel. The United States democratic allies and partners in Asia offer proof of concept of at least one alternative approach.

Although Taiwan and South Korea have employed some surveillance technology, in general, their measures have three key features that help protect against government abuse, which could serve as principles to guide future action in addition to those mentioned by previous panelists this morning.

Those technologies have been limited in scope; they have been temporary; and they have been subject to active, quick democratic oversight and review, either via the judicial or legislative branches of government.

The United States and other democracies should actively coordinate to promote a democratic vision together. To do that, however, the United States must first articulate and implement its own

strategy described above.

We must outline which forums should set standards for which technologies internationally; what those standards and safeguards should look like for each set of technologies under consideration; how interagency efforts within the United States government should be organized and coordinated; and how the U.S. should work with allies, partners and international organizations to collaboratively, but assertively, shape a global regulatory environment that is compatible with liberal and democratic values.

Given existing global demand for Chinese surveillance technology, the strategy should also consider how to address U.S. concerns while also incorporating the legitimate interests of countries that have received and are using Chinese technology.

And finally it should discuss how to handle cases where messaging on surveillance technology may run up against competing U.S. policy imperatives and priorities.

In closing, I urge the Commission to continue its important work with partners in the U.S. government, the technology sector, civil society, and around the world to develop a comprehensive long-term strategy that can capably address the risks and challenges posed by the proliferation of surveillance technology in China and worldwide.

I look forward to your questions. Thank you.

CHAIR MANCHIN: Thank you.

Yes, so much to think about, and so we sort of round [audio interference]--in this round. Lobsang.

MR. SITHER: Thank you. I would like to thank the Commission for giving me the opportunity to testify on behalf of Tibetans inside Tibet whose voices are censored and surveilled.

I'm honored to be able to share examples of religious persecution inside Tibet and how technology is used by the government of China to restrict religious freedom.

On July 6, the world celebrated the birthday of His Holiness the Dalai Lama and good wishes for him were posted on social media all over the globe. Yet, around the same time, two Tibetan artists--lyricist Khadro Tsetan and singer Tsego--were arrested in Tibet for musical tribute dedicated to His Holiness that they had shared on social media. They were sentenced to seven and three years in prison respectively.

His Holiness is the spiritual leader of the Tibetan people, but for decades the government of China has banned his photo and teachings. This is like saying you can be Catholic as long as you don't acknowledge the existence of the pope.

This ban takes many forms. In 2017, Tibetans from inside Tibet were restricted from attending the Kalachakra led by His Holiness in India, one of the most important Buddhist teachings. At the same time, research conducted by Citizen Lab at the University of Toronto showed that WeChat was censoring keywords related to Kalachakra, even the word "Bodhgaya," the location

of the teaching, in Hindi.

The research that the Tibet Action Institute conducted in 2016 showed that every video uploaded to Youku, which is the Chinese video sharing platform, similar to YouTube, with content that included the Dalai Lama was censored almost instantly, and beyond this, even videos that have content related to Tibetan language and culture were restricted completely.

And side-by-side tests that we did of some benign videos with titles and descriptions in Tibetan, Chinese and English showed the that the ones in Tibetan were more heavily censored.

Today we wouldn't even be able to conduct this research because real name registration for Chinese platform means accounts must be connected to a name and phone number registered in China or Tibet. This makes it easier for Chinese authorities to censor and surveil Tibetans and others, and almost impossible to be anonymous online.

With the passage of the Chinese

Cybersecurity Law in 2017, we are also now witnessing a proactive attempt by Chinese authorities to change global norms around freedom of expression and access to information. This includes placing demands on foreign-based companies that want to operate in areas controlled by the government of China. This results in restrictions on religious freedom and basic human rights under the guise of local law compliance.

A very concerning example of this are the ongoing actions of Apple. At the order of Chinese authorities, and at times even proactively, Apple has removed or refused to publish thousands of apps from China's version of the App Store, with little to no transparency.

This includes virtual private networks, VPNs, and news apps like The New York Times. Since Apple's closed ecosystem forces users to rely on the App Store for app installation, these removals have a huge impact, helping iOS users in China, Tibet, East Turkestan and possibly soon Hong Kong locked behind China's Great Firewall.

Apple's executives frequently insist freedom of expression and privacy are fundamental human rights, most recently calling for a more just world for everyone. While removing apps from the App Store, they say they are simply complying with local laws and regulations, but, in effect, Apple is enabling the Chinese authorities to curb, actively curb people's ability to freely practice their religion, access information and express themselves, and in doing so is violating fundamental human rights.

Research that we conducted with the organization GreatFire showed 29 Tibetan apps were censored on the Chinese App store. The majority of the censored apps were related to Buddhism, and any app with "Dalai Lama" in the title is likely to be censored.

Another concern is iFlytek, a Chinese artificial intelligence company which specializes in voice-to-text transcription and has been collecting data from Tibetan users for years without stating that--they had an app, but they

didn't say that it was run by iFlytek.

This company created an app which allows Tibetans with various regional dialects to convert speech-to-text. In a 2019 report, the company states that 60 percent of its profits come from "projects involving government subsidies," raising serious concerns about how this data is being used.

For example, we are starting to receive reports that voice conversations on WeChat are being censored. An example that I can share is in a WeChat group that I know of, a Tibetan living in exile in the diaspora was talking about, "oh, I'm going to the temple to go for a teaching of His Holiness." And a Tibetan inside Tibet didn't see the message at all so kind of like partitioning the WeChat users in Tibet and globally.

In addition, in 2018, the Massachusetts Institute of Computer Science and Artificial Intelligence Laboratory signed a five-year research collaboration agreement with iFlyTek, bringing some of the best minds from the U.S. together with the Chinese company that is likely to be involved in

censorship and surveillance.

In closing, there must be repercussions on the international stage for the harmful actions of Chinese companies that are operating globally. iFlyTek and others must face consequences for their unethical and dangerous ethnic profiling of Tibetans, Uyghurs, and other marginalized people. This holds true as well as for companies like WeChat and TikTok that are expanding their censorship and surveillance beyond China's borders, helping Beijing erode global human rights standards.

And recent research that was conducted by Citizen Lab shows that WeChat is actually surveilling users, not in Tibet or China, but globally, and using that data to censor users inside Tibet and China.

TikTok has recently been banned in India, but at the same time has showed content moderation and censorship which is following Chinese law, not the law where they operate.

I believe, as many of the other panelists

have already mentioned, that U.S.-based companies like Apple and others operating in or collaborating with China must be held accountable for their actions.

To address this, I think U.S. government and this Commission can and should bring together stakeholders, such as government officials, corporations, and people from affected communities, to draw up a code of conduct required for U.S. companies and institutions operating in China, a code that reflects the principles of fundamental human rights, including religious freedom and freedom of expression.

By joining together, stakeholders will be able to more effectively create and implement such requirements for corporations and ultimately create enough leverage that they can pressure the Chinese government to comply with such a code of conduct.

Thank you for your time.

CHAIR MANCHIN: Thank you so much, Lobsang, and now I know that there are many questions.

I will begin the questions and then certainly encourage our commissioners. I think I throw this question out to Professor Greitens, but certainly any of the panelists that would want to address this, but it certainly seems that from each of our panelists, we have talked about international standards, an international strategy, to deal with the new technologies, surveillance technology, and how we can balance the positive side of surveillance technology with the certainly criminal activity in some cases that's going on.

The United States is obviously the one that is going to have to take the lead on pushing for international standards. But, Professor, how do you see this working? Do we work through the UN? I mean USCIRF uses international standards to define religious freedom. So how do we go about being the leader in setting up or starting to develop international standards around surveillance technology?

DR. GREITENS: Thank you.

That's a terrific question, and I'm sure

my answer will be only partial, and I'd invite a couple of the other panelists to jump in because I know they have thought about this as well and done a lot of work on it.

I think the key for the United States is to recognize that this is probably an exercise for multiple departments or agencies in the U.S. government and multiple international fora. So, yes, I would encourage working with the United Nations, in particular the ITU, the International Telecommunications Union, and to look at the standards that are being submitted there.

As of December of last year, the majority of standards that had been submitted to the ITU had come from Chinese tech companies, and about half of those had been adopted earlier this spring.

So the standards are being set. It's just that the United States does not appear to be exercising as much global leadership as I think we need to to ensure that the standards that are set are compatible with American values and interests.

The other point that I would add in terms

of thinking about international leadership is that we need to be careful not to do a sort of one-size-fits-all message on this. And by that I mean it's very easy for the United States, which is really focused on technology and the threats from China's use of technology, both strategically and from a human rights and democracy perspective, to make all of its messaging about China.

And I actually think that would be a mistake because what I see in my research on the global adoption of Chinese surveillance technology is that there are democracies that are adopting this technology, and they put in their own legal frameworks to think about questions like data privacy, about, you know, civil liberties and data management.

And so we see that there are democracies that have adopted this technology, and in at least some of those cases, that's because China has offered its public safety technology, in particular, so a platform like the Safe City technology, which was mentioned earlier, by Vice

Chair Bhargava, in Central Asia; right?

We've also seen that technology widely adopted in Latin America because there are real problems with violent urban crime. Very high homicide rates are one of the predictive factors for adopting a Safe City platform.

And that suggests to me that to reinforce what Chris said earlier that we really do need to think about the recipient countries and why they're adopting technology because the United States needs to provide a compelling alternative vision, and so we need to talk to our partners about--and countries that we have various types of relationships with around the planet--about why they have chosen to adopt Chinese surveillance technology; what safeguards they can put in place themselves; and what alternatives they might be willing to consider if they adopted the technology because they simply didn't know where else to go to solve a pressing governance problem.

I know that Amy has done a lot of work on this at CSIS as well so I'd love to hear her answer

to this question as well.

MS. LEHR: If it's okay, then I will step in on that question and maybe just point to a few examples of where there's already processes that have started.

So my work has been particularly focused on facial recognition, but that really takes you into the world of AI and machine learning and so forth. So the EU has actually done quite a lot of work in this space. I mean first of all they have, they have a standard on privacy, and that alone is incredibly important. It's not enough, but it's a start.

But they also have various bodies that are developing initial guidelines for specific technologies as well as for AI broadly, and so I think looking there at what they've done, it's all grounded in human rights and global frameworks, and so I think it's really useful and quite thoughtful.

The OECD also is doing a lot of work in this space. They have specific projects on particular types of emerging technology as well as

AI as a whole.

The Office of the High Commissioner on Human Rights actually has a new project on B-Tech is what they're calling, but it's on beneficial, theoretically beneficial technology and making sure the right human rights safeguards are put in place. So those are my former colleagues actually running that program, and I have hope that that will be productive and constructive.

And then last, you just see these other kinds of alliances coming between like-minded countries to try to start setting standards, and my personal view is like all of them that are grounded in international frameworks, the U.S. should be engaging on, and we'll see, you know, which one ends up being the winner. But what I think we'll see is convergence.

CHAIR MANCHIN: Vice Chair Perkins, do you, or Bhargava, do either one of you have questions you'd like to present?

VICE CHAIR PERKINS: Yes, I have one, one question, kind of following up Professor Greitens,

and you made reference to the fact that 80 countries have been identified as using this technology. And I was curious what percentage, or do we have knowledge of how, how many of those countries are using those for harmful purposes when it comes to religious freedom?

And, you know, I think this shows the magnitude of the problem and how far it's spread that now it will be difficult to get the cat back in the bag, so to speak. And so the regulatory structure, the guidance, I think, is underscored here as a necessity.

DR. GREITENS: Thank you, sir.

Yes, we do--the written testimony that I'll submit for the record has a map of the countries in question so you can take a look, and I'd be happy to send you further information if that's helpful for the Commission's purposes.

Two brief points on that. Both democracies and autocracies and sort of hybrid regimes in the middle have adopted this technology. And so the purposes to which it is put depend less

on the technology and much more on the legal standards and human rights standards that are used to govern its implementation, and that's why these standard-setting and regulatory frameworks are so important. It's important that they be set internationally and that they be translated into national law, as my colleague mentioned earlier.

The other thing I'll say is simply to agree with your point, that it's going to be very difficult to put the cat completely back in the bag.

In the work that I've done, we have not found any case where a country that has adopted Chinese surveillance technology for policing has completely de-adopted it under public pressure. So where we've seen pushback, in Malta, in the Philippines, in other countries, there have been modifications to the laws and the standards around the use of the technology, but the technology platform itself has not been removed from the country.

I think that's an important data point to

realize as we think about what the future might look like. And I hope that answers your question, and I'm happy to follow up with further information to the extent that it's helpful.

VICE CHAIR PERKINS: I appreciate that. I look forward to looking at that map to see in particular what countries are using this, but I do think that this point underscores the urgency of moving forward with international standards.

So, thank you.

Chair Manchin, that's all I have. Thank you.

VICE CHAIR BHARGAVA: Chair Manchin, I have a few questions, which I'll make very brief.

I want to pose this to all of our panelists, and whoever wants to take them, although they come from different, different pieces of your testimony.

First, to the question of mandatory human rights due diligence, we talked about investment mechanisms, and so whether it be pension funds, universities, VCs, private equity, I'm wondering

whether there's a way in which to have those kinds of standards at the front end in the world of due diligence and making sure that you're actually implementing them versus putting the regulator on the back end because I think it creates a situation which doesn't always end up being one where everyone is realizing this is part of what you do to do business?

The second question I had was related to the way in which these technologies are playing out by race. The UN Special Rapporteur on Racism Tendayi Achiume just put out a report on racism in digital tech, and so there's obviously the problems of the ways in which these kinds of technologies are targeting people by race and ethnicity, but there's also the problems that Joy Buolamwini and others at MIT and elsewhere have looked at in terms of the fact that it just doesn't work well for people with different racial backgrounds.

And so I wanted to ask you if you had any additional thoughts on that front?

And the third is to the way in which COVID

and the public health crisis has accelerated the surveilling state both in China in different ways but also around the world, and I wanted to see if there was any, any thoughts and suggestions you had on how we can address public health as a new foundation for expansion of the surveilling state and to combat some of that?

Thank you.

MS. LEHR: I can come in on the first question and just lightly touch the second one, and then hand it off to someone else if that works.

So on mandatory human rights due diligence, I think by putting it in a law and laying out like what that process looks like, it makes it a lot more likely that companies will implement it and start to make decisions based on it. And so the fact that you either have a regulator at the end or a potential lawsuit, there's different ways of establishing responsibility or liability. I think the fact that that happens at the end doesn't mean there wouldn't be work up-front, right, after it becomes clear

that there are consequences when you don't do that work.

And so I don't see a way of getting around that. I think it's around you set the framework. You say there's an expectation, and that if you don't follow it, and there are adverse impacts as a result, you're going to be responsible in some concrete way that actually matters. So that would just be my thought on that.

In terms of the questions around racial discrimination and technology, obviously there's a lot of research on bias, and others may want to pick that up more, but I think one of the most interesting things we saw when we were looking at facial recognition around the world was that there have been actually efforts to have third parties review police use of live facial recognition in the UK, for example, and what they found was that it just doesn't work.

So when you think about human rights tests of necessity, for example, and proportionality, it doesn't pass those kind of tests; right? It's

unclear you need a facial recognition for the end, and not only that, it simply doesn't serve the purpose. So I'll let others pick up on some of the more nuanced data around bias.

Thank you.

DR. GREITENS: If I could, I'll speak to that question directly then and continue that part of the conversation.

Vice Chair Bhargava, you mentioned the issues with algorithm bias and either false positives or failure to identify or bias of various types in the types of technology that we're seeing, and I think it's important to recognize that the effort to think through those issues is going to be largely on the United States and like-minded partners and allies for the simple reason that the very fact that the technology and the doctrine that's used in China is preventive, right, means that there's no real such thing as a false positive.

It doesn't, it doesn't really make sense to think of it in those terms because you are by

definition already targeting people before they've shown any sign of politically problematic behavior. And so I think that's a task that's going to be squarely on the United States and its democratic partners and allies around the world.

The other thing I'll say about the technology is that we see a lot of media coverage that emphasizes the sort of the omniscience or the speed of this technology, and we have to remember that the goal of the Chinese Party State is partly to convince people that it's infallible and all capable.

And so for any media folks who are listening to this, I guess I would just caution that we shouldn't do the Chinese government's deterrent work for it, and it's important to actually recognize that these systems aren't perfect, that the errors have costs to human life.

But we also shouldn't talk as if this is a perfect system because then everyone will be afraid of it, and that produces exactly the effect that the CCP in some ways is trying for.

And final point about public health is simply that I think there's a much needed urgency for an active conversation with places like Taiwan, South Korea, places that have implemented systems that follow the principles that I mentioned earlier, and that have had some success in combating the coronavirus, and I think those conversations and promoting that kind of vision would be a great place to start.

And then Vice Chair Perkins, finally to your question earlier, I do have an ongoing research project looking at the effect of the introduction of Chinese surveillance technology, and I'd be happy to provide that information to you later, looking at whether or not it contributes to democratic backsliding and violations of religious freedom. So, again, when that work is done, hopefully in the next few months, I'd be happy to share it.

Thank you.

VICE CHAIR PERKINS: Great. Thank you very much.

MR. SITHER: So I just wanted to add one thing, address the fact that like in terms of like whether it's a framework or a legal requirement in the U.S., I think what has to be really considered is the fact that in 2017 when the Chinese Cybersecurity Law and the National Intelligence Law passed, that created a lot of issues in terms of how can a U.S. company in compliance with the U.S. law or in compliance with the Chinese law?

So I think there is a real need to get a lot of these different stakeholders, whether all the different U.S. companies or institutions, together to actually figure out how you can actually change some of those laws because I think there is a definite space for that because recently when TikTok was banned, they started moving out of Hong Kong because they knew that they couldn't really comply with the security, the new security law in Hong Kong.

So I think there are certain spaces to do that, and I think that's a really important space of where we have to change that law first because

otherwise it is against the Chinese law, and a lot of the companies and venture capitalists or any group will always mention adherence to a local law is an important part of how they do business.

So without changing the law, I think it does--how we do that I think is through multilateral approaches or with different like stakeholders getting together, draft and create that code of conduct that ultimately are the law.

Thank you.

CHAIR MANCHIN: Did that answer your question, Commissioner Bhargava?

VICE CHAIR BHARGAVA: Yes, and I know the other commissioners have many so let's turn to them.

CHAIR MANCHIN: Thank you.

Commissioner Turkel.

COMMISSIONER TURKEL: Thank you. Thank you, Chair Manchin. I'd like to thank our witnesses for sharing their expertise and wisdom with us.

We talk a lot about what the federal

government or international community, what our partners should do. I'd like to hear about your insights and possibly recommendations on what municipal governments should do.

Recently San Francisco stopped using facial recognition because there was no governance, specific guidance put in place. After 9/11, we gave up a lot of privacies and now we're seeing this has been expanded. So I worry that this will become a new norm, and municipalities, local government look at it on purely cost/benefit analysis and adopting this technology being promoted by the Chinese government.

And then the other question that I have is what employees of these technology companies could or should do to stop this from spreading. And also what its citizens, ordinary citizens, could do to counter this spread of digital authoritarianism?

At the end of the day, this is a threat to democracy. This is a threat to privacy. Just, you know, we've been hearing about how Chinese technologies threatening the lives of the people

around the world. Actually they're here already.

Because of the IJOP, that one of the witnesses mentioned, the Uyghur citizens of the United States cannot talk to their parents, their loved ones, freely, comfortably. Some of them made a conscious decision to cut off contacts because they don't want their family members to be in trouble in China.

So if you could comment on that, it would be appreciated. Thank you.

DR. MESEROLE: I can speak briefly to what some of the tech employees can do, which is I think one thing that's underappreciated within the public sector and political discourse on this issue is that one of the biggest constraints on technology companies is actually their employee base.

The recruitment, the tech, the market for tech talent is so fierce, particularly coming AI, retaining and recruiting top-tier talent is probably the most, probably the most significant constraint that the major tech companies we have in this country face.

And I think they've demonstrated--I think they've discovered the power that they have in that regard. I think what happened with Google is testimony to that, and I expect that that's going to continue going forward.

I'll leave it to the other panelists to answer some of your other questions as well.

COMMISSIONER TURKEL: Thank you.

MS. LEHR: Maybe I can come in for a moment on the municipalities question that you asked, Nury.

So, so we've been looking a bit at what municipalities are doing, not just in the U.S., but other places because in many countries, including, for example, the UK, police forces, for example, law enforcement is often governed at a municipal level, and so you do see some interesting examples where when certain kinds of AI systems are rolled out for the purpose of law enforcement, they're creating these multidisciplinary oversight boards, for example.

I believe the West Midlands Police did a

really interesting pilot of this that's seen as one of the better examples we have, not that it's perfect. But generally I think this is an area where there would be an opportunity to really start raising awareness in the U.S., and that might be a role you all can play in terms of just having police departments understand the imperfections of these tools and the risks they pose. And if they really feel like they have to use them, what are the kinds of oversight mechanisms they need to have in place to do that in a way that maintains public trust? That would be my suggestion.

MR. SITHER: Just to get on that, I think one of the things is I think the U.S. has to be--in some ways, I think this Commission and the U.S. government has to be a beacon in some ways to show how you can actually use surveillance.

I really don't like the word "surveillance," but at least how to use some of these technologies to actually, whether it's for policing or where there are some real uses of these because I think the issue right now is the fact

that a lot of the, I think like AI, or artificial intelligence, or like a lot of these technologies are going to China because there are no ethical boundaries.

I think one of the main boosters of the AI in China, basically what he said was we don't have to go by ethical standards so it allows them to explore everything, which is a huge challenge for us. At the same time, with technology, without ethical boundaries sometimes allows you to do kind of explore a lot more. So I think there is a space for the U.S. to actually be kind of like proactive and actually be the leader in this space in terms of how you make laws and how you make kind of like whatever is, whether it's municipal corporations and stuff like that.

And on the second point, in terms of like how, I think Amy and Professor Greitens, both of you mentioned a bit, is the fact that a lot of these technologies don't work as well, and I think that has to be really understood as well because I think it is leading to a lot of self-censorship.

If you look at like, for example, one thing in the Tibetan community that we have noticed is a lot of the Tibetans communicating with Tibetans inside Tibet or in the diaspora, there's a lot of like self-censorship of what you can or cannot say, and that raises the issue of what is, what can or can't you say at a specific given point of time because the border or the gray area always shifts.

So every time like maybe you can't talk about religion or maybe you can't talk about His Holiness, maybe you can't talk about internment of Uyghur Muslims, but can you talk about your language, can you talk about your culture, but tomorrow that may not be allowed.

So the more you self-censor, I think the more kind of like the line gets pushed, and I think also the fear that how big these surveillance tools work and how good they are or like how bad they are, I think it's also important part to understand, that they are not all encompassing, and I think that's an important part from a research

perspective to understand as well.

CHAIR MANCHIN: I want to thank everyone today. Our time has very quickly expired for us. We are at 11:30, but I know there are other questions.

Johnnie, do you have a question very quickly that you would like to ask? We could use them for some questions.

COMMISSIONER MOORE: Yeah, Chair Manchin, if you'd indulge, I think you ought to offer me and Commissioner Bauer one question, and perhaps everyone can answer succinctly--if everyone is okay with that.

I'll ask mine, and by the way I have lots of questions. You know I've got questions about China enabling Iran, you know, in the present deal that's being negotiated between the countries.

I've got questions about China's responsibility when it comes to COVID-19, you know, if this technology did enable them to know more than they're saying?

I've got a long--you know, the Hong Kong

law demonstrating to China's intent on applying their law to any dissident whatsoever anywhere in the world and how does technology enable that? But I'll leave it to one very simple question.

We are having this hearing on Cisco Webex, which is used by the United States Senate, which is used by CNN in virtually every interview they do anywhere around the world. You know, I--allegedly Cisco was involved in helping build the Great Firewall of China, and is that true or is it not true?

And I just thought it would be a wonderful opportunity to grant our panelists, each and every one, an opportunity to name any companies they would like to name that they're concerned about in the United States. That's my question.

CHAIR MANCHIN: Don't everyone speak up at once.

MR. SITHER: I can start. So, yes, so I mean like, in terms of like Cisco, I think we at Tibet Action, we have actually started using an Open Source Jitsi Meet after all the Zoom

revelations. So we actually host our own like Jitsi Meet for all these communications and stuff like that. So maybe I think there's a space for more Open Source technologies in the U.S., whether it's in the Senate or whether it's in different media outlets.

To name a company, I just want to name Apple because I think there is like more than 300 million users, and they have moved the iCloud data to China. They've given the iCloud encryption data to a Chinese company called GCBD.

So I think there are some serious implications, and then actual lack of transparency around a lot of those raises serious questions.

DR. MESEROLE: One quick thing I would just add is that American companies are in China for three very different reasons. One is access to their research. A lot of the cutting edge talent comes from China. Another is the market. China is a massive market. And the third is supply chains.

And so I think if we're going to start kind of trying to regulate American companies'

behavior in China, one thing I haven't seen much of in prior conversations about is nuance around each of those three kind of domains and reasons for why they're there because what to do about it is really going to vary significantly and we need to be able--

COMMISSIONER MOORE: Is there a company that you would like to name? I mean is there a company that you're concerned about that has enabled something or that--I just want to make sure everybody has had the opportunity. If there's a single company that's causing you the greatest concern right now in this specific area?

DR. MESEROLE: Most American companies to my knowledge are not actually operating in Xinjiang willingly. I think it's more that they're embedded in China, and their research is going into like algorithms that places like iFlytek are then using.

So I'd be worried about American researchers at Google and Microsoft, potentially working with partners in China to develop Open Source algorithms that then get ported into that

software. But I would say that that's also a more nuanced conversation than I think I can do in kind of ten seconds here unfortunately.

DR. GREITENS: Commissioner, I think you asked a question that it would take us another hearing to probably go through, and I like Chris' way of breaking down the three reasons companies are in China.

My own expertise is more on academic involvement in research in China so I'll punt that question for now and just say that I hope the Commission takes it up in detail in a future hearing.

CHAIR MANCHIN: Commissioner Bauer, do you have a final question for this? And I think the Professor adequately said this is going to call for another hearing.

But, Gary, do you have a final question?

COMMISSIONER BAUER: Let's start the other hearing right now while we have some momentum. But great testimony, very informative, and maybe I'm being a little bit redundant here.

Over the last 30 years, there's been a fever in the corporate suites of America, this dream that trade with China was going to change China, and by the way, we're all going to get rich in the process.

And I think it's been shown to have been an empty dream, and there's a lot of damage from it, but I still wonder, you know, has the fever broken because it seems like Chinese, Communist Chinese tentacles still reach into the universities, with the Confucius Institutes? You watch CNBC, the capitalist TV network that follows the stock market, more often than not guests are still being apologists for Communist China.

I'm just wondering whether anybody would want to address whether they are optimistic or pessimistic about whether we can extract this Chinese Communist influence from American economic life, educational life, and cultural life that we seem to still have a big problem with?

DR. GREITENS: Commissioner, let me just briefly speak to higher education since you

mentioned that.

I know that I've seen in the last four or five years a real debate among scholars who work in and on the People's Republic of China about our own ethics and our responsibilities as China has changed and gone in a less open and less liberal direction under Xi Jinping.

And so I'm actually encouraged that I see those conversations. I'd like them to happen faster, but often what I see is that people are trying very deliberately to maintain engagement with the Chinese people, many of whom are friends and colleagues, and some of whom have suffered greatly due to taking courageous stances or simply for pursuing free academic inquiry.

And I think that's important to keep in mind and to bring into the conversation in this hearing.

There is obviously a need for vigilance. We've seen, you know, too many cases. The FBI investigations that have come to light have turned up some serious issues, particularly in science and

technology, but I would also say that the approach in higher education should be sector specific because while it's important to prevent illicit technology or knowledge transfer to China and the Chinese Communist Party, it's also important that we understand how China's political system is changing, what its priorities are, and how it's implemented, and I think actually shutting off all academic exchange and particularly social science research to understand what's happening in China would be counterproductive to the national security of the United States.

And so I hope that our approach to higher education can distinguish between different fields and disciplines and figure out how to do that in a way that makes American national security stronger.

So thank you.

DR. MESEROLE: I was just going to add on the economic side, I think one of the reasons Apple--I would also kind of agree that Apple in terms of what it's done in Hong Kong and Tibet, you know, I would like to see them take a little bit

stronger stance against China.

But the reason they're not doing it is they're producing ten iPhones every second within China, and they don't have the infrastructure to do that elsewhere.

I do think going forward I see a lot of companies trying to, they're not going to be able to move their supply chains completely out of China, but I think they are going to diminish the risk by opening up greater capacity elsewhere. I think that's a cause for optimism.

One thing on the disentangling front, I hope we do it smartly, and especially with export controls. I think we've seen in the past where we've blocked the sale of like Intel's processors to China. They have their own kind of internal chips that can replicate what that does so it doesn't really do much, but it causes some damage.

I think it's much smarter to move upstream like China really struggles to build the machines that build processors. We can block those because those are only produced by democratic countries.

I think we can be a lot more targeted in how we're trying to disentangle so that we're kind of, you know, we're not kind of as fully entangled as we have been, but we're also not completely disentangled either, which I think would be problematic for a variety of reasons.

I think we need to be very smart about how we approach that, that process going forward.

MR. SITHER: Commissioner Bauer, I think I really want to commend you for bringing up the Confucius Institutes because I think that's a huge aspect of China's kind of like global outreach in some ways in terms of like changing the norms around what China is.

At the same time, I think if you look at like, I feel a bit more positive things are changing because I think COVID-19 actually made the world realize two important things. One, censorship does really pay an issue in terms of how you deal with issues because I think the research that Citizen Lab actually did, which was like released in March, actually showed that COVID-19,

like kind of like coronavirus terms were actually censored towards the end of December, not like in January or February so that was research that they did that actually showed terms were being censored in the beginning of, towards the end of December in 2019.

Another aspect of this fact was I think as some of the panelists already mentioned is the supply chain aspect where it is a huge lack of supply chain that actually showed whether it's through the pharmaceutical industries or whether it's like the PPEs. So I think it was shown there's an actual issue can happen.

So I think there is space that things are changing. Because otherwise like if you look at like a couple months ago or maybe even a year ago, what happened when Hong Kong, when one of the--I forgot the name of the team, the NBA team tweeted about Hong Kong, and how many, what happened there.

And so I think there were like certain things that happened in terms of like where there's too much kowtowing to the Chinese, whether it's

like a lot of the global companies changing Taiwan into China, and a lot of issues about like the flag or whatever, the Apple flag, where they removed the Taiwanese flag from Apple; right.

So anyways, but I think there is some more positive measures right now because I think we are seeing the impact during this time of COVID-19.

COMMISSIONER BAUER: Thank you.

CHAIR MANCHIN: Yes. Again, I want to take this opportunity to thank our commissioners certainly for attending the hearing today. I want to thank our panelists, who certainly have brought forth not only a great deal of information but a great deal of questions still to be answered.

And I certainly want to thank our staff, USCIRF, Jamie. I think that not only the commissioners but our panelists here are saying this is a discussion that needs to be continued, and so I will close today by saying, again, that it's not our purpose, it was not our purpose today to judge the morality of our new and emerging technologies. They certainly have great benefits

and can be harnessed for the good of society.

Unfortunately, that's not what we are seeing in China, and so anything that poses a threat to democracy, that certainly poses a threat to our freedom in religion, of human rights, then I do believe that the United States should be and always has been the beacon of leadership. And I would certainly hope that we continue to be that beacon of leadership [audio distorted]--all the entities involved, that we can provide the oversight to halt the certainly horrific activities of the Communist Party with [audio distorted] acquiring the technology can be and should be very beneficial to all of us.

But again to our panelists, thank you. Undersecretary Hull, acting Undersecretary Hull, Amy, Professor Greitens, Chris and Lobsang, thank you so much for your passion and work and for the information that you shared with us today. I guess I will turn it over to you. I hope we haven't gone too far over our schedule.

[Whereupon, at 11:47 a.m., the hearing was

adjourned.]