AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

TECHNO-AUTHORITARIANISM: PLATFORM FOR REPRESSION IN CHINA AND ABROAD

HEARING

BEFORE THE

CONGRESSIONAL-EXECUTIVE COMMISSION ON CHINA

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

NOVEMBER 17, 2021

Printed for the use of the Congressional-Executive Commission on China

Available at www.cecc.gov or www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

46–147 PDF WASHINGTON : 2022

CONGRESSIONAL-EXECUTIVE COMMISSION ON CHINA

LEGISLATIVE BRANCH COMMISSIONERS

Senate

JEFF MERKLEY, Oregon, *Chair*
DIANNE FEINSTEIN, California
MARCO RUBIO, Florida
JAMES LANKFORD, Oklahoma
TOM COTTON, Arkansas
STEVE DAINES, Montana
ANGUS KING, Maine
JON OSSOFF, Georgia

House

JAMES P. MCGOVERN, Massachusetts, *Co-chair*
CHRISTOPHER SMITH, New Jersey
THOMAS SUOZZI, New York
TOM MALINOWSKI, New Jersey
BRIAN MAST, Florida
VICKY HARTZLER, Missouri
RASHIDA TLAIB, Michigan
JENNIFER WEXTON, Virginia
MICHELLE STEEL, California

EXECUTIVE BRANCH COMMISSIONERS

Not yet appointed

MATT SQUERI, *Staff Director*
TODD STEIN, *Deputy Staff Director*

CONTENTS

STATEMENTS

	Page
Opening Statement of Hon. Jeff Merkley, a U.S. Senator from Oregon; Chair, Congressional-Executive Commission on China	1
Statement of Hon. James P. McGovern, a U.S. Representative from Massachusetts; Co-chair, Congressional-Executive Commission on China	2
Statement of Hon. Chris Smith, a U.S. Representative from New Jersey	3
Cain, Geoffrey, author of "The Perfect Police State: An Undercover Odyssey into China's Terrifying Surveillance Dystopia of the Future"	5
Hoffman, Samantha, Senior Analyst, Australian Strategic Policy Institute	7
Wang, Yaqiu, Senior Researcher on China, Human Rights Watch	9
Hillman, Jonathan, Senior Fellow, Center for Strategic and International Studies	10

APPENDIX

PREPARED STATEMENTS

Geoffrey Cain	36
Samantha Hoffman	39
Yaqiu Wang	44
Jonathan Hillman	46
Merkley, Hon. Jeff	53
McGovern, Hon. James P.	54

SUBMISSIONS FOR THE RECORD

CECC Truth in Testimony Disclosure Form	55
Witness Biographies	57

TECHNO-AUTHORITARIANISM: PLATFORM FOR REPRESSION IN CHINA AND ABROAD

WEDNESDAY, NOVEMBER 17, 2021

CONGRESSIONAL-EXECUTIVE
COMMISSION ON CHINA,
Washington, DC.

The hearing was convened, pursuant to notice, at 10:30 a.m. in Room 106, Dirksen Senate Office Building, Senator Jeff Merkley, Chair, presiding.

Also present: Representative James P. McGovern, Co-chair, Senators Lankford, King, and Ossoff, and Representatives Smith, Steel, Suozzi, and Wexton.

OPENING STATEMENT OF HON. JEFF MERKLEY, A U.S. SENATOR FROM OREGON; CHAIR, CONGRESSIONAL-EXECUTIVE COMMISSION ON CHINA

Chair MERKLEY. Good morning. Today's hearing of the Congressional-Executive Commission on China entitled "Techno-Authoritarianism: Platform for Repression in China and Abroad," will come to order. This hearing will explore China's role in embracing technology-enhanced authoritarianism and promoting its spread around the world.

In China and around the globe, we are seeing that the same technology that drives the global economy, facilitates communication, enables financial flows, and provides the conveniences of modern life can also be used for repression. Without proper guardrails to protect privacy and basic human rights, technology can control populations, trample freedom of expression, and undermine institutions of democratic governance. For the Chinese government and Chinese Communist Party, it starts at home.

Over many years, the Commission has documented the development of what has become the most pervasive surveillance state the world has ever seen. Authorities embrace technologies such as artificial intelligence, blockchain, and cloud computing—the building blocks of the modern economy—to impose political and social control of targeted populations. These technologies offer the government an unprecedented degree of control, enabled by the collection of massive amounts of data from cellphones, from personal computers, DNA, security cameras, and more.

Nowhere do we see this more tragically than in the Xinjiang Uyghur Autonomous Region. Today we will hear testimony outlining the extent of the surveillance in Xinjiang, as well as the heart-wrenching toll on individuals and their communities. We will also hear from expert witnesses who will shed light on the use of

technology in mainland China and abroad, for legitimate purposes of government efficiency and digital connectivity but also to spread the web of repressive control to cities across China, regions across China, the developing world, and even the Chinese diaspora community in the United States.

This adds up to a complex picture. The technologies we will hear about have dual-use potential, to be used for good or for ill. Many countries to which China exports surveillance systems and elements of the so-called safe cities model embrace these technologies out of a desire to combat crime or reduce traffic or provide municipal services. Yet these technologies, this high-tech authoritarianism, can be used to strip rights and dignity from millions of people across the planet.

Acting to defend freedom and to defend democracy will require the establishment of norms for the proper use and boundaries of this technology, but we can't stop there. We have to work with defenders of freedom across the globe to develop attractive and affordable alternatives. This won't be easy. That's why Co-chairman McGovern and I have convened this hearing. We need to hear from experts on how Congress, the United States Government, and the international community can address these difficult challenges.

Just as the United States confronts limitations in its ability to shape the behavior of the Chinese government, so too will we face limitations in shaping the rest of the world, especially when it comes to technology that empowers everyday life. That's why we need smart action in concert with a coalition of partners. I look forward to the testimony today to help us work to identify the approaches that can harness technology in a way that respects, rather than endangers, fundamental human rights.

I'd now like to recognize my co-chairman Congressman McGovern for his opening remarks, and that will be followed by Congressman Smith, who is joining us electronically.

STATEMENT OF HON. JAMES P. MCGOVERN, A U.S. REPRESENTATIVE FROM MASSACHUSETTS; CO-CHAIR, CONGRESSIONAL-EXECUTIVE COMMISSION ON CHINA

Co-chair MCGOVERN. Well, thank you, Chairman Merkley. Thank you for convening this hearing on the Chinese government's use of technology and digital platforms to expand and export its repressive policies. You know, where there was once optimism that the internet and new technologies would create a more open, democratized global commons, there is now a cloud of darkness. Anti-democratic and authoritarian governments have learned to harness such technology as a means to assert social control. This is no longer just about human rights abuses suffered by people over there. It is about the risks we now face from the phones in our pockets.

Take TikTok. It is immensely popular in the United States and can be a lot of fun, or so my kids tell me. It was developed by a Chinese company, and there is nothing inherently wrong with that. But we hear reports that videos on topics sensitive to its government are blocked or disappear. Americans deserve to know whether China's censorship regime is intruding on their daily lives. This concern is why the Commission, under my chairmanship in the last

Congress, expanded its reporting to include human rights violations in the United States and globally.

Our soon-to-be-released annual report will document how the Chinese government silences criticism, chills the expression of political views, and undermines international norms. The Commission's next hearing will look at the economic coercion aspect of this trend. We cannot forget that the Chinese government's techno-authoritarianism is felt most gravely by the Uyghurs and other Turkic Muslims. The surveillance regime that they have set up in Xinjiang is the most advanced and enveloping in the world. Is this the model for the rest of China and the world?

This is the key question that we hope today's witnesses will address: How can the United States ensure that its exports do not abet the spread of the surveillance state? Can we harness international partners? And how do individuals make sound consumer choices? We are addressing an immensely complicated and technical set of issues, and I'm pleased that our witnesses bring a breadth of expertise to these evolving challenges. I hope you will continue to share your research with us. Thank you, Mr. Chairman, and I look forward to hearing the testimony of our witnesses.

Chair MERKLEY. Congressman Smith.

STATEMENT OF HON. CHRIS SMITH, A U.S. REPRESENTATIVE FROM NEW JERSEY

Representative SMITH. Thank you very much, Mr. Chairman, and thank you for convening this very, very important hearing. As we all know, the Silk Road was a network of trade routes connecting the East and West from roughly two centuries before Christ to the 18th century—a transformational route in the development of the civilizations not only of China, but also the rest of the world. Likewise, the Great Wall of China was built not only for defense of China's borders, but for the regulation as well as the encouragement of trade. In short, these twin legacies of Chinese civilization have contributed much to the greater development of the world through open and transparent exchanges of goods and ideas.

Unfortunately, China under Xi Jinping and the Chinese Communist Party has not continued this proud tradition. Instead of the Great Wall that once protected its citizens while ensuring robust exchanges with the world, the Great Firewall now prevents Chinese citizens from global engagement through one of the most extensive internet censorship systems the world has ever seen. Similarly, China's Digital Silk Road is not a modern version of the Silk Road, but an intrusive ecosystem of internet architecture and surveillance technology aiming to expand the People's Republic of China's influence around the world.

Sadly, the surveillance facilitated by such tools is a fact of life for Chinese citizens, and increasingly for those who live in countries that have adopted Chinese technology. Chinese authorities' relentless persecution of predominantly Muslim Uyghurs, Kazakhs, and other Central Asian people in the country's Xinjiang region provides a disturbing preview of these tools' misuse on an even broader scale. Residents are tracked through surveillance drones, ubiquitous street cameras, and the obligatory spyware apps on their phones.

As we all know, many of those who practice a religious faith, including Christians in their churches, are now subjected to ever-increasing amounts of surveillance. Even China's COVID–19 tracking systems and apps that are supposed to protect its citizens are instead used to categorize them via different color codes according to their health status and other personal data, which are then shared with the police. This is not dystopian fiction, "1984." This is China today.

Shockingly, U.S. companies have been complicit in helping China build this techno-totalitarian state. In 2006, as you may know, Mr. Chairman, I chaired a hearing where the representatives of Google, Cisco, Yahoo, and Microsoft testified as to their role in assisting the repression in China. The year before, Yahoo had shared information with China's secret police that led to the arrest and a 10-year jail sentence of cyber dissident Shi Tao. Yahoo also handed over data regarding one of its users, Li Zhi, who had criticized corrupt local Chinese Communist Party officials in an online discussion, for which he was sentenced to eight years in prison.

We have now also seen companies like Thermo Fisher Scientific provide equipment to security services in China for a reputed genetic surveillance program. That was stated in the company's 2019 announcement that it would stop selling its equipment in Xinjiang in 2019, amid concerns raised by scientists, human rights groups, and our Commission that the authorities could use the tools to build systems to track people. The New York Times recently reported that Thermo Fisher equipment continues to be sold to police in Xinjiang.

American companies such as Thermo Fisher Scientific, not to mention those companies who subsidize China's genocide Olympics that was the subject of a few hearings that were held by this Commission and by the Lantos Human Rights Commission, often tout their commitment to corporate social responsibility principles. Such virtue signaling is now commonplace and is a form of marketing. Corporate social responsibility, however, starts with U.S. global businesses recognizing that their sales of technology products to China for use by China and its allies furthers the interests of the government of China, and often against its own people. Instead of virtue signaling, they should take a stand against Chinese human rights abuses.

If we fail to affirm our foundational American principles, including our commitment to freedom of expression and speech, I fear that the digital authoritarianism of China will become the new reality, increasingly, for all of us. Thank you, Chairman. I yield back.

Chair MERKLEY. Thank you very much, Congressman Smith.

I'd now like to introduce our panel. Geoffrey Cain is an award-winning foreign correspondent, author, technologist, and scholar of East and Central Asia. He is the author, most recently, of "The Perfect Police State: An Undercover Odyssey into China's Terrifying Surveillance Dystopia of the Future." He's written for The Economist, the Wall Street Journal, Time magazine, Foreign Policy, The New Republic, and The Nation.

Samantha Hoffman is a senior analyst at the Australia Policy Institute. Her work explores the domestic and global implications of the Chinese Communist Party's approach to state security, offering

new ways of thinking about how to respond to China's pursuit of artificial intelligence and big data-enabled capabilities to augment political and social control.

Yaqiu Wang is a senior researcher on China at Human Rights Watch, working on issues including internet censorship, freedom of expression, protection of civil society and human rights defenders, and women's rights. Her articles have appeared in Foreign Policy, The Atlantic, the Washington Post, and elsewhere. She has provided commentary to BBC, CNN, the New York Times, and others.

Jonathan Hillman is a senior fellow at the Center for Strategic and International Studies and the director of the Reconnecting Asia Project, one of the most extensive open-source databases tracking China's Belt and Road Initiative. He is the author of "The Digital Silk Road: China's Quest to Wire the World and Win the Future." Prior to joining CSIS, he served as a policy advisor at the Office of the U.S. Trade Representative.

Now I'll ask the witnesses to deliver their testimony for five minutes each, in the following order: Mr. Cain, Dr. Hoffman, Ms. Wang, and then Mr. Hillman.

Mr. Cain, the floor is yours, and welcome.

STATEMENT OF GEOFFREY CAIN, AUTHOR OF "THE PERFECT POLICE STATE: AN UNDERCOVER ODYSSEY INTO CHINA'S TERRIFYING SURVEILLANCE DYSTOPIA OF THE FUTURE"

Mr. CAIN. Chairman Merkley, Co-chairman McGovern, and members of the Commission, thank you, and it is an honor to be invited to testify here today on China's surveillance apparatus and the threat that it poses globally. Democracies around the world are straddled with a grave and unprecedented problem, the creation of new totalitarian surveillance technologies, developed faster than we can implement the democratic laws, norms, and checks and balances that will ensure that these technologies do not fall into the wrong hands.

Today I will talk about a place where these technologies have enabled genocide and crimes against humanity. I will talk about the situation of the Uyghur population in China's western region of Xinjiang, where about 1.8 million people have languished in a network of hundreds of extrajudicial concentration camps, out of an ethnic minority population of about 11 million people. That's about one-tenth of the minority population.

Since 2016, the People's Republic of China has engaged in an unprecedented experiment in social control in this region. It has deployed novel technologies in artificial intelligence, facial recognition, voice recognition, and biometric data collection to oppress its people in new and novel ways. In the 20th century, genocides took place in gas chambers and mass graves. But in the 21st century, modern technology has allowed the People's Republic of China to commit the beginnings of a genocide, wiping out a people in silence, through cultural erasure and forced sterilization. This all comes without the use of mass physical violence and mass killings.

This is all documented in my book, "The Perfect Police State: An Undercover Odyssey into China's Terrifying Surveillance Dystopia of the Future," published in June 2020 by the Hachette Book Group. From August 2017 to February 2021, I was an investigative

journalist in China, Turkey, and Kyrgyzstan, where I interviewed 168 Uyghur and Kazakh and other refugees from different ethnic minorities. These refugees consisted of former concentration camp detainees, their family members, American and European diplomats tracking the atrocities, former Chinese government officials, academics, former Uyghur technology employees at major Chinese corporations, and former Uyghur intelligence operatives from the Ministry of State Security, a powerful body in China.

In December 2017, I made my final visit to Kashgar, the Uyghur heartland, and Urumqi, the regional capital of Xinjiang. Within three days, I was detained and asked to leave. To protect my data, my sources, and my own safety, I have not returned. Uyghur and Kazakh refugees in interviews all told similar stories about the region's descent into a total surveillance dystopia. Most commonly, they recounted how authorities from the Ministry of Public Security, the Ministry of State Security, and numerous Chinese technology firms such as Huawei, Hikvision, SenseTime, Megvii, and many others have innovated the technologies that are deployed for a dragnet.

The police then use these technologies for what interviewees said was a system of mass psychological torture. When refugees and former camp detainees say "psychological torture," they mean the feeling of constantly being watched, not by humans, but by crude software algorithms designed to predict future crimes and acts of terrorism with great inaccuracy. The software platform, known as the IJOP, or the Integrated Joint Operations Platform, gathers data from a myriad of sources, including police human input, camera surveillance, and criminal and court histories, according to these former technology workers. For them, it was straight out of the science fiction dystopias that they saw once they had left the region, including "Minority Report," the film with Tom Cruise about a pre-crime unit that arrests and brainwashes people, accusing them of future crimes that have never happened.

These former technology workers told me about how the system worked from the inside of the Chinese surveillance apparatus. They said that artificial intelligence used data to train a crude, simple algorithm and find correlations between data points, and would then match up a number of unrelated, outside factors to determine whether people would commit a crime in the future. The system would then send a bump or nudge to the smartphones of local police to investigate and detain an individual for reasons often unclear to the human police using the software. These reasons for detention could be as far-flung as whether they went through the front or back door, whether they began a physical exercise routine suddenly, or whether they've had the flu and were simply late for work that day.

Without a human to oversee these decisions, refugees said they were terrified at the prospect of doing anything that departed from their daily schedules and might flag them as potential criminals. They trained themselves to become like machines or robots, able to answer every question from the police in a preprogrammed way, repressing their own feelings, thoughts, and desires in the process. These psychological tactics have been well documented at the network of concentration camps that now exist in the region of

Xinjiang. Refugees who have been there have described their fellow detainees as lacking personality or expression, as if they had had a memory wipe.

Their only way of surviving was to do what the camp guards and teachers told them, without question. The surveillance technology was designed to force them to deny their own reality and internalize the thinking of the Chinese Communist Party. By internalizing this propaganda, these detainees did exactly what the apparatus wanted of them and that was to erase their own internal sense of culture, heritage, community, and upbringing which separated them and their culture from the dominant Han Chinese population.

With that, there is certainly much that we can do to tackle this problem. I am aware of time, so I will hand over the floor to the next speaker. Thank you.

Chair MERKLEY. Thank you very much, Mr. Cain.

And now we're going to turn to Samantha Hoffman, who is joining us from Australia. Welcome.

STATEMENT OF SAMANTHA HOFFMAN, SENIOR ANALYST, AUSTRALIAN STRATEGIC POLICY INSTITUTE

Ms. HOFFMAN. Thank you, Chairman Merkley, Co-chair McGovern, and members of the Commission. Thank you for the opportunity to speak today on this important topic.

I'd like to begin with a brief explanation of what I think the appropriate definition of techno-authoritarianism is, which is that when we're talking about authoritarian technology, we are really talking about the ways that technology is attached to existing methods of political and social control, and economic management as well, in the PRC. So oftentimes while we tend to focus on the most coercive applications of technology, we sometimes tend to overlook the more everyday applications of technology and the way that that enhances authoritarian power as well.

With that, I'd like to go over three core assessments and offer some policy recommendations. I'd like to note that throughout my testimony I offer some charts that help to explain the concepts I'll go over. And I'm happy to answer more in Q&A.

So, the core assessments. First, assumptions that liberal democracy would automatically be strengthened, and authoritarians would automatically be weakened when the world became digitally interconnected have been proven false. Democracies are not going to self-correct in response to the problems created by authoritarian applications of technology. Competing with China in this space—it's not simply about winning or losing a race in terms of R&D of emerging and critical technologies such as AI or data science and storage technologies. Leadership in R&D in these areas is essential, not least to guarantee supply chain resilience, but just as consequential is the competition taking place in the conceptual space. So for the United States and like-minded countries to stay ahead, they must innovate in thinking about use cases in order to also set boundaries, so that these technologies can positively affect society without also undermining liberal democratic values.

Second, the ability to identify and protect strategic data will become an increasingly complex and vital national security task, es-

pecially under the conditions of China's military-civil fusion strategy. Knowing how particular datasets are collected and used by foreign adversaries, and imagining potential use cases, will be an essential part of ranking which datasets should be prioritized for protection. Developing effective countermeasures requires understanding the implications of the fact that the Chinese party-state conceives of the usefulness of data in a strategic competition in ways that go beyond traditional intelligence collection.

Finally, we cannot measure risk based on today's capabilities alone. Technology evolves on a trajectory. To develop effective policy responses requires assuming that the challenges China faces today in realizing the optimal outcomes of the application of technology to its authoritarian governance may not be as significant in the future, as the concepts increasingly catch up with capabilities.

The areas of policy I think we need to focus on, I think that we oftentimes—too often offer prescriptive solutions, when actually we haven't clearly identified the problem yet. So with that, I'd like to recommend for U.S. policy that time be spent to recalibrate data security policy and privacy frameworks to account for the fact of the Chinese party-state's use of data to reinforce its political monopoly. Oftentimes, companies and governments assume that their data and privacy regulations share the same goals as the other, which isn't true when it comes to the Chinese party-state and PRC companies. Even if common vocabularies are used or if some policy drivers are similar, in the PRC, unlike in liberal democracies, data security and privacy concepts—including legislation on data security in the personal information protection law recently—reinforce the party-state's monopoly on power. So companies and governments—the United States included—need to recognize this risk and calibrate their policies to account for it.

Second, the United States should collaborate with like-minded countries to develop systems for improving risk-based approaches to improving the regulation of data transfers. Organizations and governments must be able to assess the value of their data and the value of that data to any party in their supply chain who may have access to it downstream.

Finally—I'm aware I'm running out of time—governments must take a multidisciplinary approach to due diligence. Governments, as well as businesses and organizations, need to develop frameworks for conducting supply-chain reviews that take into account country-specific policy drivers. Developing such a framework shouldn't be limited to just assessing the vendor's risk of exposure to political risk. It should also include detailed analysis of the downstream actors who have access to the vendor's data. And it must include analysis of things such as the broader data ecosystem of which they're a part and the obligations that the vendors within that ecosystem have to their governments. Taking this more holistic approach to due diligence will better ensure that data can be protected in a more effective way.

Thank you for the opportunity to speak today.

Chair MERKLEY. Thank you so much, Ms. Hoffman.

And now we're going to turn to Yaqiu Wang. Welcome.

STATEMENT OF YAQIU WANG, SENIOR RESEARCHER ON CHINA, HUMAN RIGHTS WATCH

Ms. WANG. Chairman Merkley, Chairman McGovern, members of the Commission, thank you for the opportunity to speak on this issue dear to my heart. I owe my presence here today to the relative internet freedom China once had, and America's commitment to freedom of information. I was born and grew up in China. As a teenager, every day I would go online and listen to Voice of America's "Special English," a news program broadcast in slow-speed English. That's how I started to learn English, and that's also how I and many others in China got information uncensored by the Chinese government.

That was 15 years ago, and Beijing has since gotten so much better at controlling the internet. It's not only that many foreign websites are blocked, that people inside China can't access websites outside of China, but also that many people from China who now live in the U.S.—with the free internet readily accessible to them—they would still go back to the censored Chinese internet to get news information.

I'd like to use my five minutes to focus on WeChat and TikTok, two Chinese apps that have a significant presence in the U.S. First and foremost, it's essential to remember that all Chinese tech companies are subject to the control of the Chinese Communist Party. The Chinese diaspora heavily relies on the super-app WeChat for information, communication, and political organizing. This heavy reliance on this one app for everything gives Beijing huge latitude to shape the diaspora's views in ways more favorable to the CCP. It allows Beijing to know a lot about the people who have left China, down to things like who is meeting whom, at what time, and where, and it also allows Beijing to potentially mobilize an important demographic in the U.S.

Earlier this year, a network of fake social media accounts linked to the Chinese government attempted, but failed, to draw Americans out to real-world protests against racial injustice. The reason we know about this is because it happened on Facebook, Twitter, and YouTube—American tech companies that are comparatively more transparent, that periodically disclose influence operations, and that are under more public scrutiny. We do not know whether similar schemes targeting the Chinese diaspora are happening on WeChat, because it's hard to do research.

Then there is TikTok, which has far, deep reach into the lives of the American public, especially young people. One thing lawmakers need to understand is that what you see on TikTok is not so much decided by who you follow, but by the company's algorithm. There is no way for outsiders to know what information is being suppressed or promoted on TikTok that is due to the Chinese government's influence. If you search the hashtag #Xinjiang, you will find many, many videos with smiling and dancing Uyghurs, but not so many videos about the camps and surveillance and the human rights suffering. Why is this the case? We don't know.

In short, there is a lot we don't know about what Chinese tech companies are doing in the U.S., what is being censored, promoted, and suppressed, and how data is being accessed, used, and shared, and to what extent it's the Chinese government that is telling them

to do these things. But we can know that and it's up to you, people in Congress, to make it happen. Congress has recently increased its scrutiny of American tech companies. Chinese tech companies' rising popularity in the U.S. and their ties to the Chinese government should give added urgency to passing laws to require tech companies to be more transparent in their operation and to protect user data.

Lastly, here I speak not as an expert but as a member of the Chinese immigrant community in America. I urge the U.S. Government to invest in Chinese language journalism and media. Making fact-based information available in our native language is one of the most effective ways to counter Beijing's malign influence. Thank you, and I look forward to your questions.

Chair MERKLEY. Thank you very much, Ms. Wang.

And we now turn to Mr. Jonathan Hillman. Welcome.

STATEMENT OF JONATHAN HILLMAN, SENIOR FELLOW, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

Mr. HILLMAN. Chairman Merkley, Chairman McGovern, members of the Commission, thank you for holding this important hearing.

Briefly, I'd like to underscore four points from my written testimony, which focuses on China's Digital Silk Road. First, China is positioning itself as the developing world's primary provider of digital infrastructure, and it stands to reap both commercial and strategic benefits in the coming years if it is uncontested. There is an urgency to China's activities, which are expanding out of necessity and opportunity. As China's tech companies face greater scrutiny in advanced economies, they are doubling down in the developing world. Huawei, for example, in recent years has signed dozens of deals with foreign governments to provide cloud infrastructure and e-government services.

There's also great demand for digital infrastructure. Nearly half of the world still lacks access to reliable internet. Africa, which has about 17 percent of the world's population, has less than 1 percent of the world's installed data center capacity. So the opportunity for growth is vast. The United States can engage with these emerging economies and benefit U.S. workers and companies, or it can allow China to cement a position of strength.

Second, security concerns, serious as they are, will not win this competition. In much of the world, cost trumps security. Competing will require expanding the availability of affordable, responsible alternatives. Consider China's "safe city" exports, which its companies claim will reduce crime, increase economic growth, and even help fight the pandemic. Those promises, packaged with financing, can give the impression that these systems will essentially pay for themselves. But we know that these systems are also vulnerable.

In addition to raising serious human rights concerns, there are basic questions about their performance or examples of systems failing or not delivering the benefits they promise. These shortcomings open the door for the United States and its allies to offer responsible alternatives. Decisionmakers in developing countries need more than a reason to say no to China's offers. They need

something to say yes to. They're looking for partners that promote development without fueling dependency.

Third, the United States has several advantages that it can leverage to compete. U.S. companies are playing catch-up in 5G in some respects, but they remain ahead in several important areas, as well as in emerging technologies that could shift the playing field in favor of U.S. interests. For example, U.S. companies are leading efforts to provide global broadband from Low Earth Orbit satellite constellations. U.S. companies offer top-quality cloud services, "smart city" systems, and data centers.

In other words, the United States already has many of the essential ingredients to compete, but in some cases it needs to do a better job of bringing those ingredients together and competing on cost. The United States has another powerful asset that China does not, a network of partners and allies. Several promising efforts are underway to mobilize and operationalize common concerns about China's digital activities and provide alternatives, including the G–7's Build Back Better World partnership, the Trilateral Infrastructure Partnership, the Blue Dot Network, and efforts through the Quad and the U.S.-EU Trade and Technology Council. All of these efforts will need resources to succeed.

Finally, Congress and the executive branch have important roles to play in helping the United States win this competition, even though this competition is often happening in the private sector. They can help sharpen the U.S. toolkit by enabling the U.S. International Development Finance Corporation to do more, expanding the U.S. Commercial Service, and updating defense partnerships to include a greater focus on technology. And they can expand the availability of affordable alternatives by making additional resources available for the Build Back Better World partnership and related allied efforts, supporting technical assistance and capacity-building programs overseas, and using trade policy to lead on digital issues.

Additional recommendations are included in my written testimony. Clearly, none of this is going to be cheap, easy, or fast, but the United States has much to offer the developing world and much to gain by expanding the availability of affordable, responsible alternatives. Thank you.

Chair MERKLEY. Thank you all very much for your testimony. We're now going to turn to opportunities for Members of Congress to ask questions. We ask you to keep your responses fairly brief and to the point so that we can get in as many questions as possible.

I will start, Mr. Cain, with your observation that individuals—for example, Uyghurs in the Xinjiang region—experience continuous monitoring by technology, and that that monitoring is directed into a system—the Integrated Joint Operations Platform—which then triggers various officials to go and question individuals. And that that can result from which door they used, whether they were late for work, whether they had changes in their physical exercise—all of which pushes people into a kind of robotic world in which they are extraordinarily careful about what they say and what they do. In addition, not just about how they conduct themselves daily but erasing their sense of culture and heritage.

What you're describing does kind of feel like it's out of a science fiction future, but it's here today and the technologies are increasing very quickly. As you look down the road, do you see China expanding the use of these technologies into additional communities within China? Are you seeing that authoritarian figures around the world are seeking out this Chinese model and technologies to be able to use these strategies within their own countries? And if so, if you could give us a couple of examples, it would be helpful.

Mr. CAIN. Certainly. Thank you. So, yes, I do wholeheartedly agree with the assessment you just gave that this does feel like a science fiction novel. When I was in Xinjiang, it truly felt as if I was walking through the George Orwell world of "1984." So, to answer the second part of your question, there has already been a widespread attempt by both Chinese technology companies, with the support of Chinese Communist Party officials, to expand the use of these technologies, often under the guise of projects called safe cities, or under the guise of fighting crime or law enforcement, but often in reality used by authoritarian governments or quasi-authoritarian governments around the world to oppress their political opponents and dissidents, and other people whom they find troublesome.

In my written testimony, I did list a few examples that have been reported in recent years. These reports picked up in 2019 and have been continuing to pick up more. This is not a problem that's ending in any way soon. To give one example here, in 2019 the government of Uzbekistan, as reported in the Wall Street Journal, announced that it was going to adopt a safe city system in its capital, Tashkent, with 883 cameras. In very Orwellian terms, the government announced that they would use these cameras and this system to "digitally manage political affairs." Just keep in mind, this is an authoritarian government with a deep history of harassing and imprisoning dissidents.

Another example is Uganda in sub-Saharan Africa. The Wall Street Journal reported in August 2019 that technicians from Huawei, the major technology firm that makes smartphones and servers, helped the government access the Facebook pages, phones, and messages of opposition bloggers who were criticizing the president. Now, Huawei did deny this allegation, but some of its employees have stated repeatedly in the press that they see their role as simply providing the technology and not necessarily following up on its political uses or human rights considerations.

Those are two examples I can name. I hope that my information answers your question. Was there anything else you would like to ask me to go over?

Chair MERKLEY. Thank you. Right now that's great. I wanted to get those examples into the record and just note that we anticipate that this will spread to additional countries where authoritarian governments are seeking to control targeted populations or their population as a whole.

I want to turn to Ms. Wang. Ms. Wang, you noted that the diaspora of China uses WeChat. I assume that this is because, one, they're familiar with it, and two, it gives them a connection to their extended family and friends back in China. But you note that one of your recommendations is that we should pursue open-source

technology that would provide people in China the ability to circumvent censorship more easily and, I assume, folks outside of China to also be able to communicate and avoid the Chinese control of that social media. What prevents China from simply blocking such alternative open-source technology? Is there a feasible technological route to bypass WeChat?

Ms. WANG. Thank you for your question. There are currently ways to bypass China's Great Firewall, but it's always a cat and mouse game. There are VPNs available, and the Chinese government blocks those VPNs. Then there are more new ways to circumvent the censorship. Then the Chinese government blocks them again. So it's always, you know, the creativity to create new ways to circumvent the censorship competing with the Chinese government's own creativity to block it. So I think in order to win this war we need more investment in those technologies. We need to get better than the Chinese government at circumventing the internet censorship.

There are investments currently by the U.S. Government on those too, but I think in previous years there were two, but they are not open-source technologies. With open-source technologies, the third party can look into those technologies to make sure they're transparent—they don't have loopholes. So if people around the world can work together—I mean, I attend those off-the-record conferences talking to app developers who have a heart for internet freedom, and they work together. And I think the U.S. Government can play a role to make this happen in a better way. Thank you.

Chair MERKLEY. Thank you very much.

Co-chair McGovern.

Co-chair MCGOVERN. Thank you.

Mr. Hillman, this month's cover story for The Atlantic, entitled "The Bad Guys Are Winning," is about an alliance of autocrats, and notes that the Saudis, the Emiratis, and the Egyptians not only detained and deported Uyghurs, but have also purchased Chinese surveillance technology. In which countries has the Chinese model of mass surveillance and censorship advanced the furthest? And what U.S. programs can promote sustainable, transparent, global infrastructure financing as alternatives to Belt and Road? And if not, are there gaps in U.S. authorities or tools that Congress could address to bolster these programs?

Mr. HILLMAN. Thank you for the question. You know, there are too many—unfortunately, too many examples to name of these safe city projects overseas. We did a study in 2018 just of Huawei's safe city projects. We found 73 agreements across 52 countries, with a lot of that activity in Asia and Africa. Pakistan, I believe, had the most agreements of any single country. I think that there is an opportunity here for the United States and its allies to offer a superior alternative. I mean, we're actually already cooperating in some ways on this technology. The city of Las Vegas has a smart city that is provided in part by Dell, a U.S. company, and by NTT, a Japanese company.

I think we need to do more, though, to set standards that are going to drive this competition—to compete at a higher level, rather than being a race to the bottom. I would love to see an allied alternative for a sustainable city that emphasizes environmental

sustainability, that emphasizes social responsibility, that emphasizes data security. We have the companies who are working in these areas. I think we need to bring it together. And we need to offer financing. I think your question about whether we can do more—does the U.S. Government have the tools it needs—is a really important question, because what we see China doing is effectively selling products that are not the best but come with low costs and financing. And that's a very attractive proposition and sometimes difficult to turn down.

One really concrete improvement that could be made is to allow the U.S. Development Finance Corporation to do more with its equity authority. That's a new authority that the DFC has, but its hands are a little bit tied right now in terms of its ability to use that authority. I think that's really one area where Congress and the executive branch could make a change that would make a difference. Thanks.

Co-chair MCGOVERN. Thank you.

Ms. Hoffman, your testimony calls for collaboration with like-minded countries to develop systems for improving risk-based approaches to improving the regulation of data transfers. Can you give us a sense of the bureaucratic landscape and challenges in this? Which department should be the lead, or does this require top-level direction from the White House?

Ms. HOFFMAN. Thank you. I think I'll first just say that the biggest issue with our current risk-based assessment is that we tend to assume that technology is either good or bad, and we look at this issue in a black and white way. But really what we're talking about with a lot of digital and data-driven technologies, certainly the ones covered in my testimony, is that they're always, in a sense, and for lack of a better term, dual use, because data derived from these technologies can be valuable for many different reasons, and it largely depends on the intent of the actor who has access to that data—what they intend to do with it.

And it could be multiple things. You could be talking about problem solving and you could talk about enhancing capacity for control. In my testimony, for instance, I give an example of technologies—or different databases, essentially, that all feed into normal, everyday problem solving, traffic management, but then also political and legal control, feeding into the national defense mobilization system. So there are a number of ways that the technologies can be used to contribute value—or these datasets can contribute value to a lot of different things at once.

So that being said, I think that this requires really a whole-of-government approach. Of course, leadership from the White House is encouraged on this issue, but I think that there's not any one particular department that can lead on this. I think that the main thing that needs to be done actually is, we need to invest in the kind of research that would allow us to decide a better metric for judging risk, because right now the way that we do that is quite black and white. We look at the security implications of technology but forget—for instance, I wrote a paper on a company called Global Telecommunications Technology, which provides translation services. But with the data that it collects—it's a company that's controlled by China's central propaganda department—it embeds

its products in Huawei and Ali Cloud and other places, it collects data in 67 languages and uses that to support propaganda. So there are different ways that we have to imagine risk. And right now we don't have the correct toolkit to be able to respond.

Co-chair MCGOVERN. Thank you. I'm going to ask one more question—I don't know if I can fit it in a minute here—but, Mr. Cain, I want to thank you for your endorsement of the Uyghur Forced Labor Prevention Act. You know, one of the challenges with ensuring that goods are not made with forced labor is the unreliability of audits, such as the administration's Xinjiang Business Advisory notes. Do you think that the extreme levels of surveillance in Xinjiang add to that unreliability? And does it mean that monitored workers are unable to speak freely about their experiences to auditors without risk of exposure?

Mr. CAIN. Yes. Yes, that is correct, and I think that this has been well documented now in numerous news sources and academic reports on the region. There is a serious problem of extreme surveillance simply overpowering whatever audit function can exist within your typical multinational or American corporation that operates in the region of Xinjiang. There have been reports already of corporate auditors being sent to the region to fulfill these audits, but they have been detained and harassed by authorities in Xinjiang.

Just on the basis of that alone, we can reasonably conclude that whatever information is being given to the auditors who might be succeeding in obtaining some degree of information, it's deeply unreliable and almost certainly covers up the fact that there is a massive problem in the region of this slavery and forced labor. I just don't quite see a way around that when you consider that the surveillance is so deep. I think that in whatever legislation is to hopefully be passed eventually, there must be a presumption—a rebuttable presumption that whatever goods or whatever exports are originating in Xinjiang have been touched by forced labor in some way.

Co-chair MCGOVERN. Thank you.

Chair MERKLEY. Congressman Smith.

Representative SMITH. Thank you very much, Mr. Chairman, and thank you to our very distinguished witnesses. Tremendous testimony. Let me just very briefly—I mentioned that hearing that I did in 2006 with Google, Microsoft, Yahoo, and Cisco. Four of them. I asked them under oath, because I swore them all in, how do they respond when somebody says they want personally identifiable information about a dissident or human rights activist? And they said they just follow orders—reminiscent of another regime going back to the 1930s. Just following orders to give up all of this information, and many people went to prison because of it. The multidecade transfer of technology that has enabled this brutal dictatorship called the Chinese Communist Party is just appalling.

Maybe our distinguished witnesses might want to speak to that New York Times piece, "China Still Buys American DNA Equipment for Xinjiang Despite Blocks." I mean, that was October 22nd, a couple of weeks ago. You know, Ms. Wang, you made some really great points about WeChat and TikTok, how they store information for at least six months. I wonder if the diaspora is in any way aware of that, that this is all being stored. You know, Google,

under a great deal of pressure, gives people the ability—at least at 18 months—to get rid of some of the information that they seem to store forever. And I'm wondering, has anybody been arrested pursuant to the information that has been stored on WeChat, or people back home harassed? Because it's just sitting there like low-hanging fruit for the ubiquitous Chinese secret police to do whatever they want.

And finally, I have a lot of questions but there's not enough time—we in a bipartisan way keep pushing for stronger enforcement, good laws. And yet I'm wondering if it's being prioritized sufficiently. You know, it's one thing to say we're all for you, we want to make sure that the internet and certainly all of these apps are not being used to track and to incarcerate, but is it being prioritized sufficiently within the U.S. Department of State—the past administration, as well as this one? I don't want to be in any way partisan because I have been unhappy with all Democrats and Republicans since Speaker Pelosi and I and others so vigorously oppose MFN without human rights conditionality. You know, you don't trade with a dictatorship and think they're somehow going to matriculate to a democracy. They get more potent and more capabilities to do wrong.

So if you could speak to those issues. Ms. Wang, maybe I'll start with you.

Ms. WANG. Thank you for your question. I'm a member of the Chinese immigrant community here. I would just simply say that it's impossible not to use WeChat to live your life. I don't have WeChat on this phone, but I have WeChat on another phone, just to separate the data. You know, for example, if I go to a Chinese restaurant, they offer a discount and that discount only exists on the app, on WeChat. You cannot get the discount through your Facebook or other social media app. I wanted to mail something back to China, and I have to use WeChat in order for this to work.

Because of that kind of ecosystem—so, you know, among immigrants in the United States, we are living here, have a job here, we communicate with each other on WeChat. Just this convenience provided by WeChat sucks us into the system. I mean, you know, the question is whether we are aware of the problem. Obviously, we know that the government censors, surveils our communication. But I think that people are just resigned to the fact that this is our way of living. I mean, I make a concerted effort—I only have WeChat on another phone. When I need to use it, I use that phone. For most people—I mean, if you just have a day job that you work as an accountant, what's the point, right?

So that allows the Chinese government to have huge latitude to collect information and shape views. You know, one good example I would give is that in the past there were local newspapers in New York, where I live, that cater to the Chinese diaspora. Now in order for the local newspapers to be read by the Chinese diaspora here, those newspapers have to go through WeChat, because people only read the news on WeChat. So in a way, the local news information catering to the Chinese diaspora has to go through Beijing censorship before it delivers to you. That is the kind of control the Chinese government is able to exert on the Chinese diaspora.

Whether there is evidence that people have been arrested because of what they say on WeChat, I mean, yes. There is a good story done by the New York Times: There is a woman who lives in Canada. She was just using WeChat, talking—I think she criticized the Chinese government. When she went back to China, she got arrested. It's all because of what she said in Canada. This is a story that is disclosed, and she is willing to talk about it. I'm sure there are many stories of people who have no awareness that their communication is being looked at, and when they go back to China, they get detained. Thank you.

Representative SMITH. Thank you, Ms. Wang. Would anybody else like to speak to the prioritization of this issue? Is it being sufficiently prioritized within the U.S. Government?

Ms. HOFFMAN. I'd be happy to speak.

Representative SMITH. Please, thank you, Dr. Hoffman.

Ms. HOFFMAN. I think, first, and just to reiterate the points that Ms. Wang just made, I know so many stories, just in interviews that I've conducted and through my own network, of people who have been harassed for their digital communications while they were overseas. And in some cases—I know of one particular disturbing case where the person concerned and their family were both permanent residents or citizens of liberal democracies. And the family, in one case, was harassed by Chinese embassy authorities about the other family member's activity online, and they were harassed in person. Sorry to be vague, but I think it's important to protect the identity of those people. And I know of other cases along similar lines, where people received threats online as well. It's a very real problem.

Now, in terms of the prioritization, I think that—I mean, I'll always say that the U.S. Government and other governments around the world aren't prioritizing these issues enough. But I will say that increasingly there is an awareness of the problem. I think that the issue is that sometimes we think that—okay, now that we're aware—we'll solve the problem, whereas I don't think we've adequately defined it yet. And that's why in my testimony I talk a little bit more about how we conceptualize the issue of tech authoritarianism.

We're not just talking about the most coercive use of technology. We're also talking about the export of normal, everyday problem-solving technologies not just to other authoritarian or illiberal regimes, but to democracies, including the United States. And so until we adequately define the problem, many policy responses that we develop aren't going to truly address the nature of the problem. And so my concern is that we're sometimes jumping ahead with solutions before we've identified the problem.

Representative SMITH. Thank you.

Ms. HOFFMAN. Thank you.

Chair MERKLEY. Thank you, Congressman.

Representative SMITH. Thanks.

Chair MERKLEY. We're now turning to Senator Lankford.

Senator LANKFORD. Mr. Chairman, thank you. Thank you to all the witnesses and for the truths that you're bringing to light. It's exceptionally helpful to be able to continue to get the facts to the forefront.

I do have some follow-up here that I want to be able to talk to Ms. Hoffman about. Mr. Hillman had mentioned there are 52 countries right now that they know of that have the "safe cities" technology. My question is, How is the Chinese government using that data in these 52 different countries that have the safe cities technology? Not how those countries are using it, how is China using that data that they're then harvesting from those 52 countries that are using the "safe cities" technology?

Mr. HILLMAN. Thanks, sir, for your question. You know, I think there's evidence—some of this is tough to study in open sources—but there's evidence to suggest that there are vulnerabilities in these projects that are putting at risk the data in the countries that are using them, and potentially giving access to that data to Chinese authorities. So for example, in Pakistan there's actually a legal case underway with a county that was involved in developing a safe city project there that alleges that it was forced to install a backdoor that would allow access to data from Beijing. There's also been examples of hardware being discovered on surveillance cameras where Pakistani engineers were not initially made aware of that hardware; you know, hardware that could allow you to gain access remotely to those systems.

So you know, we see these examples of data challenges. You know, there's another good example in Papua New Guinea, which borrowed money from China and allowed Huawei to build a data center there. When a third party did a study of that data center, the conclusion that they reached was that the security was so poorly designed that it was probably intentionally designed that way. So I think that there's ample signs to be concerned about some of the espionage risk. There's also, in some cases, a commercial incentive for China's large providers of surveillance equipment to collect data on foreign populations so that they can improve their algorithms and the ability of their algorithms to recognize foreign faces, for example.

Sometimes I've heard just anecdotally that giving access to that data might result in getting some preferential financing for the project. So there's both an intelligence concern here as well as a potential commercial angle for some of the Chinese companies that are involved.

Senator LANKFORD. Ms. Hoffman, do you want to add to that?

Ms. HOFFMAN. Yes, thank you. One issue that I'd like to cover is the way that Chinese companies can draw value out of data without any sort of malicious disruption or break-in, because I think oftentimes we focus on the risk of espionage with PRC technologies. But the other part we miss is that with a company—any company, like Huawei, Alibaba, others—they are providing a service. And at the same time, you know, it depends on who sits within their supply chain. There could be automatic access to the kinds of data that they collect. That's described in my written testimony. It's the first figure I think that helps to explain that concept a little bit more. But then it's also the concept that I described in a paper from 2019 called "Engineering Global Consent" about the propaganda department company I mentioned earlier.

Now, that being said, I think that the recent Data Security Law as well as the Personal Information Protection Law in the PRC fur-

ther illustrate what we already know about the way that the Chinese party-state can exert pressure on companies and other individuals and entities to access data whenever it chooses. So in particular, the Data Security Law says that data security in China is governed by the state security concept, which is ultimately about the party-state's political security. And that's what makes it different from national security. And it also says in article 2 of the law that data handling activities taking place outside the PRC, when those activities are seen to harm state security, or the public interest and the lawful rights and interests of citizens and organizations in the PRC, then they can be pursued for legal responsibility in accordance with the law.

Now, what could be harming state security? Well, that could be the political opponents of the CCP we were discussing earlier. But it could be anything that the party-state sees as potentially undermining its power, and so essentially there are no limits to the party-state's power in this case. Companies might say, Well, we don't want to hand over data, we're not going to do that. But ultimately, if they're operating in the PRC and they're based in the PRC, they're bound by PRC law.

Senator LANKFORD. So if there is a company that's a Chinese-owned company that's a "privately owned," non-state-owned company that's functioning in the United States or in any other country, and they're sending data back to China, that data can be owned and can be captured then by the Chinese government, or the actions of that company can be overseen by the Chinese government, correct?

Ms. HOFFMAN. Yes.

Senator LANKFORD. Ms. Wang, there's been a lot of conversation about a social score for Chinese citizens—that in the surveillance state that they live under, that they're all graded internally and receive some sort of score even to get access to mass transportation, to jobs, to moving, to being able to have the ability to travel overseas. What do you know about this social scoring of individuals in China?

Ms. WANG. The social credit score system, in its current form it's mostly a blacklist. So, for example, if you have not fulfilled your obligations, such as, you know, you had a loan that you didn't pay on time, then you would be on this list and then it would affect your daily life. When you go to the train station you cannot buy a ticket because of your record of not paying a loan. And it doesn't only affect you. It also affects your family. And there are instances where children cannot be enrolled in the school system because their parents have not paid a loan. So it's like punishment—guilty by association.

I mean, currently the data has not been integrated. In different localities there are different systems. And it is the Chinese government's ultimate goal to have all the data integrated into one giant database so they can have access to it, and no matter where you're based, take it and exact punishment against you based on whatever things you have done. I mean, look at the health code that was developed during COVID—right now, this health code is being used against political dissidents and human rights lawyers because you have to have the code to travel. It has to be a green code. But

as a human rights lawyer, you are here for the past few months; you have done nothing. And you have a red code. And, you know, it's a health code. It shows that you are a health risk. But this has nothing to do with your actual health situation. It's entirely that you're a human rights lawyer and now you have a red code, and you cannot travel.

So the point is that the government can construe it as, "We try to build a social credit system that is for the good of society," but it can be used in other ways, to carry out their political goals. Thank you.

Chair MERKLEY. Thank you very much. We're now going to turn to Congresswoman Steel, to be followed by Senator King, and then Congressman Suozzi, and then Senator Ossoff.

Congresswoman Steel.

Representative STEEL. Thank you, Mr. Chairman. Thank you very much, and thank you to all the witnesses for coming out today because this is a very important issue. China continues to shape and abuse the global rule-based system and China cannot be a transparent world leader and continue to strip Hong Kong's rightful freedoms and autonomy and allow forced labor in the Xinjiang Uyghur Autonomous Region, and world leaders cannot continue to allow China to abuse its own citizens and threaten those who live in other countries, too.

So all the witnesses, whoever can answer these questions—and I'm just so grateful for that—the United States called China out for their abuses in development of a 5G network. Yet, many U.S. companies are investing in China's semiconductor industry. So what threat does that pose? And what message does that send to the rest of the world? If any witness can answer, I'm grateful.

Mr. CAIN. So, yes, without a doubt the problem of major multinational corporations and American corporations investing in the Chinese semiconductor industry, which is heavily state backed, which has the enormous support of various state coalitions and bodies within China, is a major threat to both American industrial and security interests. This is something that, speaking more historically, there has long been an American business interest in investing in East Asian semiconductor markets. Japan was the original one, then South Korea, Taiwan, and now the People's Republic of China is trying to build its own semiconductor industry. And this has been going on for about two decades now. It's one of the core technologies to ensuring that these surveillance technologies can actually function.

But I would just like to point out that there is a bill that has been on the floor already—let me just double check—I think it was the House, yes, introduced in 2020, the CHIPS for America Act, which is H.R. 7178. You know, I read the legislation. I thought it was very well written. It was a bill that I came upon in my own research. You know, it was just something that popped up, and I think it does do potentially great work because it offers subsidies and investments to ensure that America can continue to produce its own semiconductors and that we can bring manufacturing home. I think this is ultimately the solution to protecting our interests and our own democracy and security from infiltration and from the meddling of the Chinese Communist Party.

Representative STEEL. Thank you very much for that answer because we have a supply chain crisis, too. Manufacturing companies coming back here and then we are building our own here. I think it's going to make life much easier, and we can stop China from abusing these businesses.

My second question is, China must abide by international laws. If they fail to do so, the U.S. and democratic partners must hold China accountable. It's very, very tough to do because they're not really transparent. So as China becomes a leader in artificial intelligence, how dangerous is this to the future threat of human rights abuse that they are doing right now? And do China's digital currency plans add to this abuse?

Ms. HOFFMAN. I'd be happy to comment on that. I did some research last year on China's digital currency and I think that's actually a great—I don't feel like I'm an expert particularly on digital currencies, but on DCEP (China's Digital Currency Electronic Payment system) I think the most interesting thing is actually the technology itself, rather than the currency, the concept of the digital yuan. I think it's the technology behind it. Now, it's all very much in development, and I think that this is an area where other countries can get ahead.

But I think that the same issue with digital currency-related technologies, as with anything else "smart cities"-related, if China is ahead in setting standards—what I tend to look at would be that domestically it's technical committees that are setting standards. And those involved—say, if you're talking about facial recognition systems that can involve the PLA, research institutes and People's Armed Police, or Ministry of Public Security research institutes, along with companies like Huawei and Dahua and others—then those technologies, when they're exported, would be used to embed those standards that are being designed within the PRC.

So in order to get ahead of any potential violations of human rights or undermining of liberal democracy, I think that's where we need to get ahead in terms of standards setting. And that's where we also need a lot more research. And DCEP is an interesting issue because it's still very much in development. So while it's not necessarily a threat today, it's potentially an issue that we will face a number of years down the line. And so getting ahead of it, from a policy perspective, is encouraged so that we don't continue with the sort of whack-a-mole approach that's been taken with companies like Huawei.

Representative STEEL. Thank you very much. I yield back.

Chair MERKLEY. Thank you very much. We'll now turn to Senator King.

Senator KING. Thank you, Mr. Chairman. This is a fascinating hearing. And I think it's interesting to note that George Orwell was right as a matter of fiction back when "1984" was written. I thought he was wrong in the '80s when the fax machine and mobile phones allowed a flowering of individual rights across the world and in fact contributed in the early part of this century to the Arab Spring. Now we're learning he was right because technology is being used aggressively for repressive purposes.

Ms. Wang, a couple of questions. Are the Chinese people aware of the level of internet censorship? Do they know they're not get-

ting the whole picture? I'm talking about ordinary people who are, you know, a clerk in a factory who goes home and goes on the internet. Do they know that they're being censored?

Ms. WANG. I think people generally have an idea, but I think the censorship in recent years has gotten so bad that, you know, people have a general awareness that "my conversation is being censored, I don't get the full picture." But they don't know exactly which information is being censored. I can speak for my family, because many members of my own family believe that COVID–19 originated from the U.S. because the Chinese government just has been so heavy on propagating this idea. It's hard to talk them out of it. And you know, they are in China. They haven't gone out of China for several years. And they don't have alternative information. And——

Senator KING. So the Chinese people are as subject to disinformation as we are?

Ms. WANG. Yes. I mean, the Chinese government has much latitude in spreading disinformation inside the country, so there's no counterinformation. They are the only spreader of disinformation.

Senator KING. So, to answer my question, you said people are somewhat aware. The second one is: Are they aware of the extent to which they're being surveilled?

Ms. WANG. I would say that people have a general idea that, in terms of specific people, people don't believe that the Chinese government would look into how you talk to your wife, until one day the government—the police summonses you saying, "You know, you were chatting with your wife; you were badmouthing the police." And then you say, "Wow, I can't believe they're looking into this." Because people just generally think, "What's the point? I'm nobody. Why are you looking at me?"

Senator KING. But they are aware?

Ms. WANG. Generally, yes. Generally. But they wouldn't think specifically. People think that the government is looking at everybody, but why me, right? It's like everybody has an equal chance of being hit by the bus. Only when you get hit by the bus do you say, "Oh, it happened to me right now."

Senator KING. So as people are gaining awareness of (A), the extent to which information is being censored, (B), the extent to which they're being fed information that may not be true by the government, and (C), that they're being surveilled, is there any resistance? Is there any resentment? Is there any—does anybody care about this?

Ms. WANG. There absolutely is resentment. One obvious example is after the early days of COVID, which, you know, spread because the Chinese government initially suppressed the information, you can just see——

Senator KING. Do people know that? Do they know that people died because of the government's actions?

Ms. WANG. Initially, yes. Yes, people are aware the local Wuhan government was suppressing information.

Senator KING. So my question is, are they angry? Are they resentful? Is there any resistance being built up? Is this developing political resistance to the surveillance state, or is it hopeless?

Ms. WANG. Well, I think initially people were very angry when COVID just happened. But then later the government was so good at disinformation. You know, they were saying, We did such a good job of trying to contain the virus, and look at America—everybody is dying. You know, it's necessary that we control the information. And people were angry at first, then they were happy with the government's control. So it's an ebb and flow. I think generally people have a kind of discontent and anger, but it's heavily suppressed.

Senator KING. Well, we have a tradition here of free speech, of the First Amendment, and sort of fierce individual liberty impulses. Is there something in Chinese history and culture that makes the Chinese people more likely to tolerate this kind of central control over their lives? Does this go back to the Han Dynasty, or—I'm trying to get at a cultural rationale for this acceptance.

Ms. WANG. I don't think it's cultural. It's entirely political. You have experienced the Cultural Revolution, the Great Famine, and millions of people died. You internalized that message: Do not criticize the government. 1989 happened. You tried to criticize the government; your body was rolled over by a tank. That's a message—do not criticize the government. And I mean, for——

Senator KING. So it's garden variety intimidation?

Ms. WANG. Yes. And I think for my generation—I'm 34 years old—or people younger than me, if you were born into a situation where you have never experienced freedom, you don't know how it feels to be free. I mean, I was born in China, and I've lived in the U.S. for over 10 years. I can feel the difference—if you have not experienced freedom, you don't know how it feels to be free.

Senator KING. Changing the subject a bit, Mr. Hillman, we've talked a lot about the spread of Chinese technology, Huawei particularly. Are any of these countries experiencing buyer's remorse? Is there a realization that they've been had, that they've given up something substantial? Or are they just happy they got a better deal?

Mr. HILLMAN. I think that there definitely are instances of buyer's remorse. We've seen a little bit of that in Pakistan. Some politicians have made comments about how—I mean, at one point, in one "safe city" project, about half the cameras weren't working. And so there are these instances of disappointment, of promises not being delivered, but it's a political challenge too, because the incentives are not really there for the leaders, the decisionmakers, that approved these systems and probably had a big ceremony around their announcement, to own up to the fact that they might not be performing.

Senator KING. Well, I'm running out of time. But if we were talking about future potential customers, is it a matter of just developing our own good server and equipment and subsidizing it like they do? Do we have to—I mean, that's inconsistent with our theory of the market, but do we have to fight fire with fire? Otherwise, we're just standing by and watching them wire the world.

Mr. HILLMAN. Yes. We need to package the parts together. We need to bring together not only the hard infrastructure but the services and training, too. Training's really attractive. And you need financing in some cases to makes this look feasible upfront and to make it competitive. As we do that, though, it's not only

about providing just a different option, but I do think we want to be offering a superior option, one that we have evidence that it works and one that comes with some safeguards, too, that are going to prevent some of the harm that we see when these systems are used in the wrong way.

Senator KING. Well, of course, part of the problem is some of these authoritarian regimes want that surveillance capacity that we may be reluctant to supply them with.

Well, thank you all very much for your testimony. This is a very important hearing. Thank you, Mr. Chairman.

Chair MERKLEY. Thank you very much, Senator King. And we'll turn to Congressman Suozzi.

Representative SUOZZI. I want to—first, this is terrifying, what's going on. And I want to thank the Chairman for sounding the alarm on this very important issue. I want to thank the witnesses for the work they've done, the books they've written, the articles they've written, the work that they've done worldwide to try to expose this. I think that the world is coming to realize that—you know, our view, ever since Nixon went to China, that the more that China was exposed to us the more they'd become like us—with democracy and capitalism—just hasn't happened. And the Uyghur situation is the worst example of their crimes against humanity, but there are so many other things—with the Tibetans and Hong Kong.

And now this use of technology is really the terrifying thing that we face. When I was in seventh grade, I remember Sister Ruth saying, You know, the world is moving so quickly these days we haven't had a chance to figure out how this is affecting us. And, you know, now things are moving at such a rapid pace, and the world doesn't realize—we don't realize how technology is affecting us in so many different ways. And I remember when we were little kids we would watch shows and they'd say, If only he'd used his genius for good instead of evil.

There are great things that are happening with technology—you know, facial recognition and voice recognition and iris recognition and gait recognition. These could all be very positive things that could be used. I use CLEAR when I go to the airport. But this is being manipulated by the Chinese Communist Party for the domination of people. And we have to expose to the world what's going on. I was very interested in Ms. Wang's comment when she said we have to get more Chinese-speaking journalists to report on this, because we have to advise people as to what's happening.

You know, it's so scary, this idea that people are changing their behavior so they don't trigger the artificial intelligence surveillance monitors; they're trying to stay very robotic. I mean, that's terrifying. We talked about the effect of WeChat on the Chinese diaspora, but there are many groups that use WeChat even beyond the Chinese diaspora. So they're monitoring that as well. And TikTok is used by everybody. And they're using that to monitor people's behavior.

I want to figure out what we can do to let the world know this is happening. I don't know how but we have to sound the alarm beyond this hearing that this is happening. I think that one of the things that Ms. Wang talked about was the use of social media to

sow civil unrest here in the United States of America. I know it's a little bit off topic, but it's so important that the American people realize that this is not just happening out there somewhere. This is invading our lives in WeChat, in TikTok, but also on other American platforms where the Chinese Communist Party, as well as the Russians and the Iranians and the North Koreans, are trying to sow civil unrest in America and elsewhere in the world, using our freedoms. Can you give us some examples of what you're aware of regarding that, Ms. Wang, of how the Chinese Communist Party is trying to sow civil unrest in America?

Ms. WANG. Well, you know, it's hard to tell because it's hard to do research. And that's one of the recommendations that was in my written submission, that we need to make those tech companies more transparent, so people know how they moderate the content, how they enforce their content moderation. You know, what kind of data they are collecting this year with the Chinese government. So there are ways to know it, and it requires the Congress to pass a law to make it a mandate.

In terms of social unrest, I would give an example of how WeChat is powerful in political organizing in the U.S. Right now, affirmative action is being—I think right now it's still in a Boston court. And this anti-affirmative action is becoming a movement, and that movement is very much initiated by the Chinese diaspora, and the organizing of that movement is primarily on WeChat. I have no evidence whether the Chinese government is interested or not, but the idea is that a very important civil rights movement in the United States, the organizing of this movement is on a platform that is controlled by the Chinese government, that can be manipulated by the Chinese government.

This is definitely a cause for concern. I mean, in terms of other protests, whether the Chinese government is playing a role, I mean, I live in New York City. There are anti-Asian racist protests, other different kinds of protests concerning the Chinese diaspora. Again, it's happening on WeChat, the organizing's on WeChat. We don't know whether the Chinese government plays a role or not. And we can know if Congress makes it happen.

Representative SUOZZI. I think it's very important—first of all, this is happening elsewhere in the world as they're trying to export their technology through the "safe cities," as you said, and the social scores and everything else. And they're trying to export the technology so they can have control of this data and build this massive database of people throughout the world. But we need to get the American people more interested in this topic.

Anything that you can do to help us understand—for example, I know that the Chinese government, the Chinese Communist Party, was doing a presentation at a Queens museum, just right outside my district, where they were completely misrepresenting the history of the Tibetan Buddhists. And the people in the community, you know, stood up and fought to get that removed. And we know how they use the Confucius Centers to spread disinformation. And I know about an example of a New York City police officer of Tibetan descent who was actually working with the Chinese Communist Party to surveil Tibetans in the area he was responsible for patrolling.

So we need to figure out how we can let people know what the Chinese government is doing—the Chinese Communist Party is doing—that's actually affecting us here in the United States now, so we can get them more and more interested in this and expose how they're trying to export these ideas, utilizing these—so anything you can just throw out there in the few minutes or few seconds I have left, I would appreciate. Anything that you can give us as examples of really abusive behavior.

Ms. Hoffman.

Ms. HOFFMAN. Yes. Thank you. I think that this is a challenging question. It's one that's been incredibly important. I mean, I think that the biggest issue that we have here is perhaps one that Ms. Wang highlighted in a previous response, which is that people tend to think that, Well, I'm not going to be affected. It's not me. It's hard to conceptualize something that is quite abstract, actually, for a lot of people. It's very real and palpable for political opponents of the CCP, but it's less obvious to you and me, for instance. And so I think part of it is that we need to have a very clear public conversation about the implications of data collection, about what it means when a——

Representative SUOZZI. I think my time has expired so I don't want to keep holding the rest of the people up. I'm sorry.

Ms. HOFFMAN. All right. I'm sorry.

Representative SUOZZI. Thank you.

Chair MERKLEY. Thank you very much, Congressman.

We'll now turn to Senator Ossoff from Georgia.

Senator OSSOFF. Thank you, Mr. Chairman, and thank you to our panel today.

Ms. Wang, you've covered some of this previously, but could you please specify with as much detail as possible the specific tools, technologies, platforms, and their manufactures and producers, that are used by the CCP to surveil and intimidate dissidents and other political opponents abroad?

Ms. WANG. I think it goes back to, you know, everybody uses WeChat, so the government has an easy way to get information on what you're doing. I chatted with people about me coming to Washington, D.C., on WeChat, and the government can get information just by reading my WeChat. Again, it's that heavy reliance on this tool gives the government a lot of latitude to do that. This is a tool that affects the diaspora. And then if you use other websites or any kind of technology developed in China, the government very much can have access to that information and use those tools to surveil you, even if you are in the United States. I don't know if that answers your question.

Senator OSSOFF. Thank you. I'd like to ask others on the panel to share their expertise on the same question, which is to specify the platforms, technologies, tools, software providers, techniques commonly used by the CCP for purposes of surveillance, intimidation, or other forms of influence projection targeting those outside of Chinese borders. We'll start with you, please, Mr. Cain.

Mr. CAIN. Yes. I actually interviewed a number of former technology workers from Huawei, SenseTime and Megvii, and also the company that runs WeChat. One of the things to first bear in mind is that two laws in China, the National Intelligence Law and the

National Security Law, passed around 2015 and 2017, I believe, essentially make it a crime to not assist the state with data that they request. That's not the exact wording, but that's essentially the spirit and the fundamentals of those particular laws.

The technology workers who I spoke with, obviously they've been out of China for a few years; they can't return. But as of 2018–2019, they can say without any doubt whatsoever that these companies do not need to rely on special cybersecurity lapses or special ways of hacking into people's phones and stealing their data. It's simply that if there's data that is passing through China, and that data is requested by the Ministry of Public Security, the Ministry of State Security, another body, the companies will turn it over. And they gave many specific examples.

You know, among my population that I was with for many years are the Uyghur population and the Kazakhs and some of the Tibetans. You know, they provided specific examples of WeChat in particular simply handing over massive amounts of data from the years 2010 to very recently, 2017–2018. Just simply every text message being stored in servers for two years at a time, and then using AI surveillance technology to attempt to find matches between data points to try to predict whether someone might become a terrorist. This AI technology was being deployed by various Chinese ministries, but WeChat was the one that voluntarily, when requested, provided this data.

So I haven't found evidence personally yet of a special backdoor system that's spying on all of us. I think it's simply the CCP asks, and the companies will follow.

Senator OSSOFF. Thank you. And continuing with you, Mr. Cain, please, how is that law enforced with respect to U.S. and multinational firms that are doing business in China, locating servers in China, selling products in China?

Mr. CAIN. So, just to clarify, you mean, Senator, the ways that we enforce the law here to prevent that from happening in China?

Senator OSSOFF. No, enforcement of the National Security and Surveillance Laws by which the Chinese government compels the disclosure of such information from WeChat for U.S. and multinational firms who are doing business in China. In what ways are they subject to such enforcement? What data, perhaps related to U.S. persons, may be disclosed or be compelled to be disclosed to the Chinese authorities on the basis of that law? And, Mr. Cain, if you'd prefer, you can feel free to defer to anyone else on the panel who may have greater expertise, or happy to hear from you on that.

Mr. CAIN. My understanding of both laws is that they do not have jurisdiction only within the People's Republic of China. It is simply that any data that is passing through a server can be requested by the authorities there. In the past I have used WeChat. I no longer use WeChat at all because the security risks have been well documented. But I have called, just experimentally, to see what happens—I have called people in Tibet. I have called people in Xinjiang. You know, this was before the terrors that exist now, when things were a little better. WeChat would show messages—would show a warning that says, You know, you are calling this region; your data is potentially not going to be protected here.

There was a little disclosure for a while. I haven't done that lately because I don't want to endanger anybody, but that was something that these software companies I think made clear and admitted—that this data is not safe.

Senator OSSOFF. Thank you, Mr. Cain, and with my remaining 45 seconds, Ms. Hoffman, the Aussie perspective on that question, please.

Ms. HOFFMAN. Thank you. Well, in a recent report called "Mapping China's Technology Giants," we highlighted on our website the privacy policies for a lot of the PRC technology companies that we mapped in this project. It's 27 companies. And one thing that we note is that it's common for all companies, globally, to state in their privacy policies that your data may be transferred to another country where you aren't residing, and that when that data is transferred, it would be governed by local law. Of course, PRC tech companies say the same. And as Mr. Cain has highlighted, when they're subject to the State Security Law and the Intelligence Law, they really don't have a choice. And they aren't even allowed to admit that they've assisted in state security in those cases.

You know, I think that the other part of your question, and one that a couple of other questions throughout the hearing have highlighted, is that we aren't just talking about the ways that political opponents of the CCP, that their data can be collected and used. We're also talking about the way that, say, U.S. citizens and other citizens around the world can have their data accessed and used. And of course, we aren't thinking as much about individuals being surveilled—of course that does happen—but it's also just about what value data has when it's aggregated.

An example that I once provided is the idea of Hisense, a smart TV provider, being a state-owned company—partly or fully state-owned, I can't remember at the moment. And, you know, smart TV data doesn't sound extremely interesting until you think about that data in the aggregate, because what's useful for advertisers would also be useful from a propaganda perspective in terms of influence operations in the future. So it's not just individuals being tracked, it's also the issue of the strategic value of aggregated datasets.

Senator OSSOFF. Thank you, Ms. Hoffman. Thank you, Mr. Chairman.

Chair MERKLEY. Thanks so much, Senator Ossoff, and now we're going to turn to Congresswoman Wexton of Virginia.

Representative WEXTON. Thank you, Mr. Chairman. I want to thank the panelists for joining us here today and for your important work in this area. You know, I represent a district here in Northern Virginia which has one of the highest populations of Uyghur Muslims outside of Xinjiang. And the stories that they tell me are terrifying, about what their families are going through back home. And you know, the surveillance doesn't end in Xinjiang or in China. They will talk about how they get a random message on WeChat saying: Do you want to talk to grandma? You know, this is somebody that they haven't been able to talk to in months. And when they set up this video call, there will be a Han Chinese member of the PRC sitting on the sofa with grandma. And it's just that kind of intimidation and threats that really are very, very frightening.

Ms. Wang, I want to thank you for all your testimony about what's happening and everything that you've been dealing with. This whole issue with WeChat is particularly frightening because it is so insidious and so ubiquitous for the Chinese diaspora and because it's not just disaggregated data; they can focus on a single individual and surveil what they are doing. So it's pretty frightening. And I want to thank you for everything that you've done to draw attention to this issue.

But I do want to talk for a minute about the Olympics, which are coming up around the corner. I'm very concerned about the PRC's use of surveillance technologies during the Olympics and what risks the athletes, in particular, will face while in China. If any of them does choose to speak out about the human rights abuses that are taking place in China nowadays, what sort of retaliatory actions can they expect from the PRC and from the Chinese government? I guess, Mr. Cain, if we could start with you on that question.

Mr. CAIN. It is alarming, I must say, just the fact that Beijing can hold an Olympics, given the state of human rights and the downward trend toward authoritarianism in the country. So when it comes to thinking about ways to raise awareness, or to boycott, or to do something to make people notice what's going on in China, I think just more broadly speaking the Olympics is the moment to do that, because this is going to be a time when all the world's eyes are going to be on China. In 2008, shortly after the Olympics, there were mass protests in Tibet and Xinjiang in 2009–2010, owing to conditions there, to human rights atrocities and a lack of civil liberties. And that was a moment—I think a rare moment in the past when the world's eyes were really on just the depth of the suffering that exists in some of these regions.

I think that naturally there's going to be a lot more attention on these problems as the Olympics approaches. I'm not totally sure given all the vested commercial interests, the big advertising deals, I think there's a feeling among many U.S. corporations and foreign companies that I've spoken with personally that we need to not be too loud about China and its own human rights problems in the interest of preserving our own market access and our advertising relationship with the Olympics. I'm not sure quite how to get around that one particular problem short of continuing to sanction foreign companies that do business in Xinjiang and with other human rights-abusing regimes. But I am optimistic in one sense, that when the Olympics does happen, there will be major broadcast coverage of the underbelly and some of the human rights atrocities now unfolding.

Representative WEXTON. Thank you. And do you think that there will be any retaliatory action as a result of that?

Mr. CAIN. I think that there already has been a good deal of retaliatory action. There has been in the past two or three years a vast clampdown, you know, both on human rights in Hong Kong and other parts of China, but also retaliation against foreign journalists who travel to China or who live in China and who have been reporting on these topics. I mean, among my own personal media circles I can count now on maybe two hands, it could even be a few dozen people actually by now, who've simply been denied

visas, or rejected, or who have lost their visas as retaliation for their reporting.

So without a doubt I do think that there will be threats from the Chinese Communist Party against major broadcast media that attempt to cover these human rights atrocities as the Olympics are underway. But I think that also the PRC has worked itself into a bit of a hole in this situation because I don't think they have much more leverage, having already yanked the visas of so many foreign journalists in the country who already speak Chinese who do great coverage of the country. Now that they've been pulled out, they're simply going to be sitting in South Korea or Japan now, simply covering these atrocities from the point of view of refugees who have escaped.

Representative WEXTON. Thank you so much, Mr. Cain. I don't think you'll get any argument from anybody on this panel. We've had a number of hearings about the Olympics and their sponsors and everything and trying to up the pressure on them in advance of those Olympics taking place.

Now, Mr. Hillman, it's clear from your presentation that U.S. firms could compete with firms from the PRC in terms of providing cutting-edge technology and those services across the globe. How can we ensure that the technologies that we're exporting aren't going to be used for surveillance technologies and to advance authoritarianism? And is the PRC currently using any U.S. technology in order to conduct its surveillance activities at home or abroad?

Mr. HILLMAN. Thanks. It's a challenging question, but I think one that we can do not only just through unilateral action but also in coordination with partners and allies. Developing principles for the use of technology—in a way some of that's being done now through the Quad, which includes the U.S., Japan, Australia, and India. I think there are similar efforts underway through the U.S.-EU Trade and Technology Council. And so not only making alternatives available but helping to provide technical assistance and training that ensures that these alternatives are being used appropriately. And then we obviously have tools and sanctions to use in instances where they're not being used appropriately.

There, unfortunately, are examples of U.S. technology, U.S. products being used. And, you know, this is something, unfortunately, that's not new. I think there's a longer history here that goes back to the 1990s and the opening of China's market, and the eagerness with which a lot of U.S. companies and other foreign firms wanted to go into that market, their willingness to form joint ventures, to share technology, and still the willingness of some companies to supply components that are needed for these systems. So I do think that that's an area that deserves more attention.

Representative WEXTON. Thank you very much. I see that my time has expired, so I'll yield back.

Chair MERKLEY. Thank you very much, Congresswoman Wexton. I appreciate your raising the Olympics. The Congressional-Executive Commission on China has tried to really amplify attention to the fact that the International Olympic Committee has placed the world's athletes in the untenable position of making them essentially complicit in China's effort to use the Olympics to paint a very

beautiful vision of their country and to basically hide the genocide that they are engaged in against the Uyghur community and other ethnic and religious minorities.

So it's important that we continue to raise it, that we encourage athletes to speak out, that we encourage sponsors to speak out, we encourage sponsors to condition any future sponsorship on massive reform by the IOC, that we protect the athletes' ability to speak freely at the Games, that we encourage network coverage, cable coverage to explore the underbelly, as referred to by our witness today, and give us an opportunity to educate the world about China's practices when those Olympics occur.

I want to address one additional topic that I don't think has really been covered today and that is the challenge that U.S. companies have in operating in China when they are compelled to hand over information. One particular example that's been well covered is Airbnb. Sean Joyce, the former chief trust officer of Airbnb, resigned in 2019 because China was requiring Airbnb to hand over not just phone numbers and email addresses, but also messages sent between guests and hosts. In other words, participate in the surveillance strategy of the country. Many other companies are compelled to share information. And it's just an ongoing challenge that needs to be highlighted.

Ms. Wang, can you bring any kind of a spotlight to bear on this challenge?

Ms. WANG. Thank you for the question. I do think this is a huge problem. You mentioned Airbnb, and there are many other companies. I think one big company is Apple. China is Apple's second-largest market and lots of people in China use iPhones. By Chinese law, Apple's data is stored in China. So basically, what you are communicating through your iPhone inside China is known to the Chinese government. The database is jointly owned by Apple and a Chinese government-controlled company.

Besides that, actually, over the years Apple has taken down over 1,000 VPNs from the Apple Store. I mean, activists are extremely frustrated. They always tell me, I cannot find a VPN in the app store to communicate, to access information blocked by China. I brought that message to Apple. They always tell me the same message—you know, we have to comply with the local law. Then I would tell them, But you have a human rights commitment; that is in your policy. How do you fulfill that human rights commitment? So there's always this back and forth.

I don't know what the solution is if Apple values its market in China so much. You know, I really want to see—there should be more awareness of Apple's complicity in human rights violations in China, because Apple has a good reputation here for its support for privacy rights. I think the public needs to be more aware of those tech companies' behavior outside of the United States.

Chair MERKLEY. Thank you. Do any of our other witnesses wish to comment on this challenge?

Mr. HILLMAN. If I could, I would just add that I think U.S. companies are not only facing that pressure within China, but increasingly in some third markets too, where they're being asked by foreign governments to provide access to their data. That pressure is increased in situations where they have a Chinese competitor who's

also operating in that market and does not hesitate to provide access to that data. So I think it's not an easy challenge to solve when your competitor is willing to engage in that race to the bottom. The U.S. does have trade tools it could use. I think we also need to, again, be working with partners and allies so that companies that are operating in our markets—you know, in the United States and the European Union in particular—are abiding by that higher set of standards.

Chair MERKLEY. Thank you very much, and I thank all of our witnesses—Mr. Cain, Dr. Hoffman, Ms. Wang, Mr. Hillman—for sharing your expertise with us today and helping us to gain a better understanding of how to combat techno-authoritarianism.

First, your testimony has portrayed a truly chilling description of techno-authoritarianism and the surveillance state, a combination of old strategies of neighbors spying on neighbors and sanctions for misbehavior combined with new technological strategies that involve the collection of information from video monitors, from internet use, cellphone use, artificial intelligence, processing of information to target specific individuals. Basically, an all-encompassing surveillance cage that turns humans into state-monitored and -controlled robots, stripped of their freedom of movement, their freedom of expression, as well as their cultural heritage.

Second, that this strategy is spreading throughout the world, through China's Belt and Road Initiative, including their safe cities program, their cybersecurity program, and through the interest of authoritarian governments in having more control over both targeted groups within their country and over their general population.

Third, that the speed of technological development and deployment is outpacing the response of democratic governments to monitor it, to understand it, to respond to it, and to set standards for it.

Fourth, that without a lot of effort, scrutiny, and action, U.S. capital and technology become complicit in supporting and accelerating this techno-authoritarianism.

Fifth, that China is using this strategy to also collect information on individuals throughout the world, including the Chinese diaspora, and that information is used to influence and control people outside of its borders.

And sixth, that responding to Chinese techno-authoritarianism is going to require a coalition of free states and the development of an alternative model of technology; that is, equipment and practices, and that it is certainly urgent for us to act.

I hope today's hearing has helped draw attention to this urgency and to the importance of the United States and other free nations engaging with international organizations that set international norms and standards, such as the International Telecommunication Union. That we be very aware of and respond to the challenge of protecting data. That we recognize the need to increase our Chinese skills, including our Chinese-language journalism, and that we help provide open-source responses to Chinese applications like WeChat. So that's a significant, challenging, and exceedingly important agenda. And I appreciate all of you for shedding light on it today. We must pay attention and we must act.

The record will remain open until the close of business on Friday, November 19th for any members who would like to submit any information for the record or additional questions for our witnesses. Thank you all so much. And with that, this hearing is adjourned.

[Whereupon, at 12:29 p.m., the hearing was concluded.]

A P P E N D I X

PREPARED STATEMENTS

PREPARED STATEMENT OF GEOFFREY CAIN

Chairman Merkley, Co-Chairman McGovern and members of the Commission, it is an honor to be invited to testify here on China's surveillance apparatus and the threat it poses globally.

Democracies around the world are straddled with a grave and unprecedented problem: the creation of new, totalitarian surveillance technologies, developed faster than we can implement the democratic laws, norms, and checks and balances that will ensure these technologies do not fall into the wrong hands.

Today I will talk about a place where these surveillance technologies have enabled genocide and crimes against humanity. I will talk about the situation of the Uyghur population in China's western region of Xinjiang, where about 1.8 million people have languished in a network of hundreds of extrajudicial concentration camps, out of an ethnic minority population of about 11 million people. Since 2016, the People's Republic of China has engaged in an unprecedented experiment in social control in Xinjiang. It has deployed novel technologies in artificial intelligence, facial recognition, voice recognition and biometric data collection to oppress its people in new ways.

In the twentieth century, genocides took place in gas chambers and mass graves. But in the twenty-first century, modern technology has allowed the People's Republic of China to commit the beginnings of genocide, wiping out a people in silence, through cultural erasure and forced sterilizations, without the use of mass physical violence and killings.

This is all documented in my book *The Perfect Police State: An Undercover Odyssey into China's Terrifying Surveillance Dystopia of the Future*, published in June 2020 by the Hachette Book Group. From August 2017 to February 2021, I was an investigative journalist in China, Turkey and Kyrgyzstan, where I interviewed 168 Uyghur and Kazakh refugees. These refugees consisted of former concentration camp detainees, their family members, American and European diplomats tracking the atrocities, Chinese government officials, academics, former Uyghur technology employees at major Chinese corporations, and former Uyghur intelligence operatives from the Ministry of State Security, an intelligence body.

In December 2017, I made my final visit to Kashgar, the Uyghur heartland, and Urumqi, the regional capital of Xinjiang. Within three days, I was detained and asked to leave. To protect my data, my sources, and my own safety, I have not returned.

TECHNOLOGY, TORTURE AND GENOCIDE

In interviews, Uyghur and Kazakh refugees all told similar stories about the region's descent into a total surveillance dystopia. First and most commonly, they recounted how authorities from the Ministry of Public Security, the Ministry of State Security, and Chinese technology firms such as Huawei, Hikvision, SenseTime, Megvii and others have innovated the technologies that are deployed for a dragnet. The police used these technologies for what interviewees say is a system of psychological torture.

When refugees and former camp detainees say "psychological torture," they meant the feeling of constantly being watched, not by humans, but by crude software systems designed to predict future crimes and acts of terrorism, with great inaccuracy. The software platform, known as the IJOP, or the Integrated Joint Operations Platform, gathered data from a myriad of sources, including police input, camera surveillance, and criminal and court histories. It was straight out of the science fiction movie *Minority Report*, about a police unit that arrests and brainwashes people believed to be future criminals before they have even committed a crime.

Former Uyghur technology workers, from major Chinese companies, told me about how the system worked from the inside. They said that the artificial intelligence used data to train a crude, simple algorithm and find correlations between data points, and then determined who was likely to commit a crime based on a number of unrelated, outside factors. The system sent a "bump" or "nudge" to the smart phones of local police to investigate or detain an individual, for reasons often unclear to the human users of the software. These reasons for detention could be as far-flung as whether or not a resident began a physical exercise routine suddenly, entered their home through the front or the back door, or had the flu and was late for work one day.

Under constant surveillance, sometimes without a human to oversee these decisions, refugees said they were terrified at the prospect of doing anything that diverged from their daily schedules and flagged them as potential criminals. They trained themselves to become like machines or robots, able to answer every police question in a pre-programmed way, repressing their own feelings, thoughts and desires.

At concentration camps, where psychological and physical torture have been well-documented, refugees described fellow detainees as lacking personality and expression, like people who had a memory wipe. Their only way of surviving was to do what the camp guards and teachers said, without question. The surveillance technology was designed to force them to deny their own reality and internalize the thinking of the Chinese Communist Party. By internalizing CCP propaganda, these detainees did exactly what the CCP wanted from them: detainees erased their own internal sense of culture, heritage, community, and upbringing which separated them from the dominant Han Chinese population.

KEY SOURCES

Looking beyond data alone, the personal stories of Uyghur and Kazakh refugees are harrowing and have much to warn us about the misuse of surveillance technologies.

To protect their safety, I granted anonymity to two key interviewees who appeared in my book. They are "Maysem," a young woman now in her thirties from Kashgar, who obtained a master's degree in the social sciences from a university in Ankara. She remains in Ankara as a refugee after being taken to a lower-level "reeducation center," followed by a high-security "detention center," in late 2016 for about one week.

Maysem asked for anonymity and for the author to obscure some details of her story because she believes her entire family has been taken to a camp as of late 2017 or early 2018, and remain vulnerable.

The other key anonymous source was "Irfan," who now resides in Turkey and had obtained a mid-senior management position as an information technology (IT) worker at a major Chinese telecommunications firm in Urumqi, his hometown. Irfan asked for anonymity because he was revealing what the PRC would probably consider state secrets, surely leading to the imprisonment of his family in Xinjiang, and his own imprisonment and perhaps even execution should he ever be required to return to China.

Under contract with the Ministry of Public Security, Irfan led teams of IT workers and engineers who, from the late 2000s and early 2010s, began establishing networks of surveillance cameras all over Urumqi. Irfan witnessed the escalating surveillance by the Ministry of Public Security firsthand. This included the rollout of dragnet artificial intelligence (AI), facial recognition and voice recognition systems, and digital surveillance camera technology from 2010 to 2015 until his departure from the telecommunications company in 2015.

Irfan also detailed the connivance, complacency and involvement of major Chinese telecommunications firms in creating the surveillance apparatus in Xinjiang. All the firms he detailed have been sanctioned by the U.S. Department of Commerce, a government body that, under both the Biden and Trump administrations, has similarly accused these firms of involvement in human rights abuses in Xinjiang.

I did not grant anonymity to interviewees who had already become public figures and whose stories were available in the public domain, search engines and media websites. One key public interviewee was Yusupjan Ahmet, who came from Karamay, Xinjiang and who had migrated to Turkey as an intelligence operative for the PRC Ministry of State Security.

Yusupjan detailed his life story in a series of hours-long, recorded interviews with the author. He stated that he intended to travel to Afghanistan in the early 2010s to become a jihadist fighter, that he was instead imprisoned, and that the state coerced him into spying on fellow Uyghurs by torturing and threatening his mother.

In 2017, with the help of a former military officer in Pakistan, Yusupjan was flown to Afghanistan where he joined a local Taliban militia, while posing as a jihadist. The Ministry of State Security ordered him to report back on the activities and whereabouts of Chinese citizens, mainly Uyghurs, who had become jihadi combatants in Afghanistan. In 2017, the Ministry of State Security relocated Yusupjan to Turkey, where he was ordered to gather intelligence on the local Uyghur community in Istanbul, Turkey. In particular, PRC intelligence operatives wanted him to infiltrate local Uyghur-owned businesses posing as a young person seeking employment.

PRC intelligence officers told Yusupjan that the Turkestan Islamic Party (TIP), a fundamentalist terror group, had infiltrated the Uyghur community in Turkey, and that his objective was to locate and document these supposedly widespread underground networks. Yusupjan, however, was disillusioned to find no evidence of widespread infiltration. He found the PRC's claims to be little more than a conspiracy theory designed to justify the mass detention of his fellow Uyghurs back in China.

In 2018, Yusupjan defected from the Ministry of State Security and went into hiding. He relocated to Zonguldak, a small industrial town in northern Turkey on the coast of the Black Sea. There, he kept a low profile, working as a gas station attendant. Two other Uyghur residents in Zonguldak told the author that while they heard, through local community talk, that Yusupjan was a resident, they knew little about him and his life story. He kept a low profile.

In November 2020, while visiting a friend in Istanbul, Yusupjan was preparing to offer an interview to the BBC. As he left his friend's apartment, a man wielding a gun, reportedly of Azeri (Azerbaijan) background, appeared on the street and shot him twice in the back of the shoulder. Yusupjan survived, but has been hospitalized, close to paralyzed and unable to walk for months.

EXPORTING THE SURVEILLANCE STATE

The technologies are no longer unique to Xinjiang. Chinese companies have made them available for export around the world, posing threats to democracy and rule of law. Mexico, Brazil, Serbia, Singapore, Turkey, Spain and South Africa are all examples of countries that have embraced "Safe Cities" programs, designed by Huawei for surveillance and crime prevention.

While there is nothing wrong with adopting technologies that can stop crime, one legitimate fear is that authoritarian or quasi-authoritarian governments will exploit these systems to seize more power and monitor their political opponents. One study by the Brookings Institution concluded, "countries that are strategically important to the PRC are comparatively more likely to adopt it, but so are countries with high crime rates."

I will give some examples. The authoritarian government of Uzbekistan, a Central Asian country between China and Russia, announced at a security meeting in May 2019 that it signed with Huawei to develop a Safe Cities system with 883 cameras in the Uzbek capital, Tashkent, to, in Orwellian terms, "digitally manage political affairs." In non-democratic Uganda in sub-Saharan Africa, *The Wall Street Journal* reported in August 2019 that Huawei technicians helped the government access the Facebook pages and phones of opposition bloggers who criticized the president. Huawei denied the allegation.

DENIALISM OF CRIMES AGAINST HUMANITY

It is a tragedy that some individuals, companies and governments have chosen to downplay or deny evidence of mass atrocities in the Xinjiang region, sometimes for their own market access to the PRC. Their denials are in line with CCP propaganda.

My research underwent a three-month, rigorous fact-checking process, looking for inconsistencies, omissions and inaccuracies. With a professional fact-checker and a journalist, we compared our own refugee testimonies with the published reports of other refugees, academics and journalists, including research by all the scholars testifying here today. We checked the locations and structures of concentration camps and other locations on Google Maps satellite imagery, in technology company press releases and official reports, and in investigative journalism already published in other periodicals such as *The New York Times, The Wall Street Journal*, and *BuzzFeed*. We also double-checked Chinese-language media.

HOW TO TAKE ACTION

Because of the situation before us, I urge Congress to take action on these points. The following are a sample of possible actions, and are not exhaustive:

- Pass the CHIPS for America Act (H.R. 7178), introduced in the House in 2020. The Act will invest in and incentivize research and development and supply chain security in America's semiconductor industry. Establishing a strong semiconductor supply chain at home, in America, will be key to stopping malign state actors from undermining our democracy through technology.
- Pass legislation that would require the U.S. Department of Commerce Bureau of Industry and Security (BIS) to publish reports on a regular basis for Congress and the public, providing evidence for sanctions of foreign businesses.

While BIS already releases reports on sanctions, sometimes they do not offer much detail as to why specific entities have been added to the sanctions list. In October 2021, BIS began amending export controls to cover items used in surveillance and espionage that disrupts networks, a great step in the right direction.

- Pass the Uyghur Forced Labor Prevention Act (H.R. 1155). A similar bill was passed in the Senate in July 2021, and H.R. 1155 has been introduced in the House but has not proceeded. The bill would pressure the PRC to curtail the Xinjiang surveillance dystopia, by blocking goods made with forced labor in Xinjiang, such as clothes and electronic components, from entering the U.S. market.

PREPARED STATEMENT OF SAMANTHA HOFFMAN

CHINA'S TECH-ENHANCED AUTHORITARIANISM

Core Assessments

1. **Assumptions that liberal democracy would automatically be strengthened and authoritarians weakened as the world became increasingly digitally interconnected have been proven false. Democracies are not going to self-correct in response to the problems created by authoritarian applications of technology.** Competing with China in this space is not about "winning" or "losing" a race in terms of R&D of emerging and critical technologies, such as AI or data science and storage technologies. Leadership in these R&D areas is essential, not least to guarantee supply chain resilience, but just as consequential is the competition taking place in the conceptual space. To stay ahead, the United States and like-minded countries must innovate thinking about use-cases, and set boundaries, so that these technologies positively affect society without liberal democratic values being undermined.

2. **The ability to identify and protect strategic data will become an increasingly complex and vital national security task, especially under the conditions of China's military-civil fusion strategy.** Knowing how particular datasets are collected and used by foreign adversaries, and imagining potential use cases, will be an essential part of ranking what datasets should be prioritized for protection. Developing effective countermeasures requires understanding the implications of the fact that the Chinese party-state conceives of the usefulness of data in a strategic competition in ways that go beyond traditional intelligence collection.

3. **We cannot measure risk based on today's capabilities alone.** Technology evolves on a trajectory, and to develop effective policy responses requires assuming that the challenges China faces today in realizing its optimal outcomes may not be significant in the future as concepts increasingly become capabilities.

What Is Tech-Enhanced Authoritarianism?

When we talk about "authoritarian technology", this should be defined as the uses of technology that enhance authoritarian power. The phrase "tech-enhanced authoritarianism" is a way of thinking about this concept that demystifies the phrase "techno-authoritarianism". Techno-authoritarianism connotes a vision of the future that, for most passive observers, is either like Huxley's *Brave New World* or Orwell's *1984*. The reality though is not like science fiction.

On one hand, we see the Chinese party-state deploying extremely coercive applications of technology, most notably in places like Xinjiang and Tibet and with public security surveillance projects like the "Sharp Eyes" or "Skynet".[1] But, elsewhere, it is technologies that provide services or enhance convenience and problem solving that allow the party-state to expand and reinforce its power. For example, data from IoT sensors can improve logistics and predictive analytics that increase supply chain visibility and efficiency in normal times, but in crisis those same technologies could facilitate defense mobilization capacity.

China's tech-enhanced authoritarianism is unique in a national context. When these technologies are exported globally, it is not necessarily the intent of an end user to use them in ways that enhance authoritarian power. Some fragile democracies or illiberal regimes import the technologies for coercive purposes, but others are genuinely seeking the best and most affordable technologies for problem-solving. With many technologies associated with tech authoritarianism appearing benign in their everyday end-use, problematic assumptions are made that undermine the risks they embed. For instance, one problematic claim that is made goes as follows: "[x]

technology or [y] system is not inherently problematic, it is applied in ways that solve ordinary governance problems, but there is a potential that in the wrong hands that it will be misused." Following the same problematic logic, some claim that if that technology is exported, "we can control the problem because we control its end-use". The problem is analysts describing "misuse" are thinking subjectively.

For the Party-state, problem-solving technologies can also enhance authoritarian control, the two are not mutually exclusive. The tendency to compartmentalise "good" and "bad" use points to a failure to conceptualise the strategic potential value of the technologies. The Chinese Party-state sets itself apart because it is setting itself up to be able to exploit that inherent dual-use at all times. This is notable in terms of how it applies PRC law to Chinese companies and in terms of how it seeks to seize advantages in the development of technical standards.

Data Security and Digital Supply Chain Security

Technologies that collect, store and transfer data facilitate the delivery of wide range of services on which society is becoming increasingly dependent. In a June 2021 report, "Mapping China's Technology Giants: Supply chains and the global data collection ecosystem,"[2] we found that existing global policy debates and subsequent policy responses concerning security in the digital supply chain miss the bigger picture because they typically prioritize the potential for disruption or malicious alterations of the supply chain. Yet, digital supply-chain risk starts at the design level. Not all methods used to acquire data need to be intrusive, subversive, covert or even illegal—they can be part of normal business data exchanges. Figure 1 illustrates how a digital supply chain can be compromised without a malicious intrusion or alteration. The data-sharing relationships that bring commercial advantages are also the same ones that could compromise an organization.

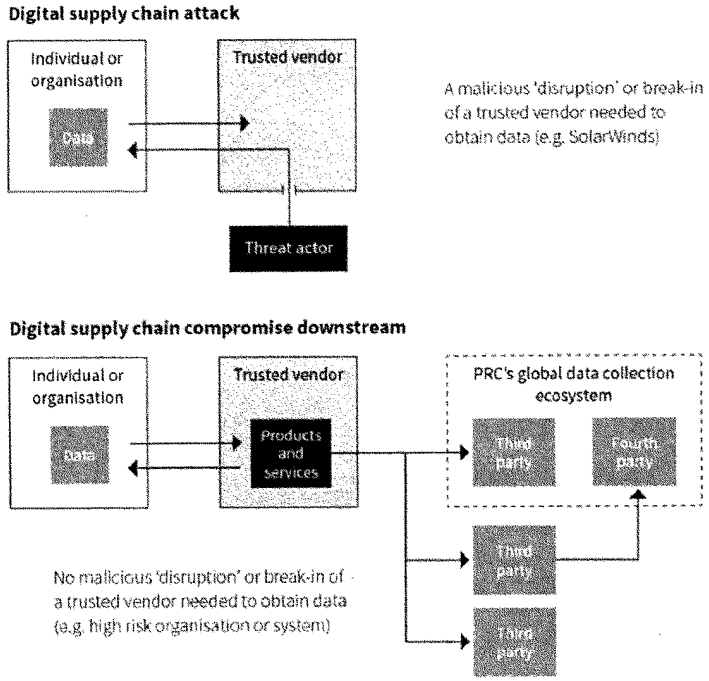

Figure 1: Dr Samantha Hoffman and Dr Nathan Attrill, "Mapping China's Tech Giants: Supply chains & the global data collection ecosystem," Australian Strategic Policy Institute, 8 June 2021: https://www.aspi.org.au/report/mapping-chinas-tech-giants-supply-chains-and-global-data-collection-ecosystem

My October 2019 ASPI report, *Engineering Global Consent*, provided a case study describing what this problem can look like in reality. The report identified and de-

scribed a machine-translation company controlled by the Central Propaganda Department, Global Tone Communications Technology (GTCOM), which engages in global bulk data collection.[3]

GTCOM claims that one of its many platforms, InsiderSoft, accumulates about 2–3 petabytes of data per year, including from Twitter and Facebook.[4] The company feeds the data it aggregates into various tools, some linked to state security. For instance, in 2017, GTCOM's Big Data Director, Liang Haoyu said: Through the real-time listening and interpretation of cross-language data, the company has established information security systems for countries and regions, and ultimately finds relevant security risks in targeted areas through open channels ... [Only with] image recognition on top of text and voices, can [we] better prevent security risks.[5]

There are strong indications that GTCOM generates military and other state security intelligence out of the data it collects (and not only because an image from GTCOM Big Data Director Liang Haoyu's aforementioned speech shows a screen claiming '90% of military-grade intelligence data can be obtained from open data analysis'). GTCOM runs the 2020 Cognitive Research Institute (the 2020 Institute), which is a mechanism through which the company does R&D to enhance 'machine learning, deep neural networks, natural language processing, speech recognition, AI chips, data mining, distributed computing'. The 2020 Institute has numerous NLP (natural language processing) algorithms, including for automatic text identification, sentiment analysis, event element extraction, sensitivity determination (whether text contains 'violent, reactionary, pornographic or other sensitive information'), relation extraction, and 'military text classification'. The 'military text classification' algorithm classifies text according to subfields such as nuclear, shipping, aviation, electronic and space.

Data and the information it helps generate can also support the party-state's development of tools for shaping public discourse. Separately from GTCOM, research funded by the National Natural Science Foundation of China, the National Key R&D Program of China and a key project of the 'National Society Science Foundation of China' has worked specifically on automatic news comment generation; that is, synthetic comments on news articles. The methodology is based on NLP and large-scale datasets of real comments in Chinese and English. Given GTCOM's Propaganda Department ownership, its state security role and the fact that it collects bulk data in 65 languages, the research indicates a potential tool that a state-controlled company such as GTCOM could use, especially given that the research was funded with national-level grants. It's also simply indicative of how GTCOM's bulk data may be used by others who have access to it, such as researchers working in cooperation with GTCOM's 2020 Institute. Other R&D associated with GTCOM may also have security implications, even if it's not immediately obvious. For instance, among GTCOM's patent applications is a machine translation method based on generative adversarial networks (GANs). GAN can be used to synthesise images based on AI or use visual speech recognition to perform lip-reading and speech output (it's the same type of technology commonly associated with synthetic media, meaning 'fake news' and 'deep fakes'). It's an intriguing patent not because of the technology itself, but because GTCOM is controlled by the Propaganda Department. The department's intent isn't simply to use GTCOM to provide language services, but to shape global public discourse.

Future Trajectory

Sometimes that control might just be about improved information integration and sharing. Integrated Joint Operations Platform is designed to help with the integration and sharing of data on citizens across multiple government agencies.[6] One metric used to identify threats is energy usage from smart electricity meters: abnormally high energy use could indicate 'illegal' activity, but such meters in their normal use would also improve the accuracy of meter readings. Another example is building datasets for use in the PRC's 'national defence mobilisation system' (a crisis response platform) using data sourced from a variety of government cloud networks, from smart cities to tourism-related cloud networks (Figure 2).

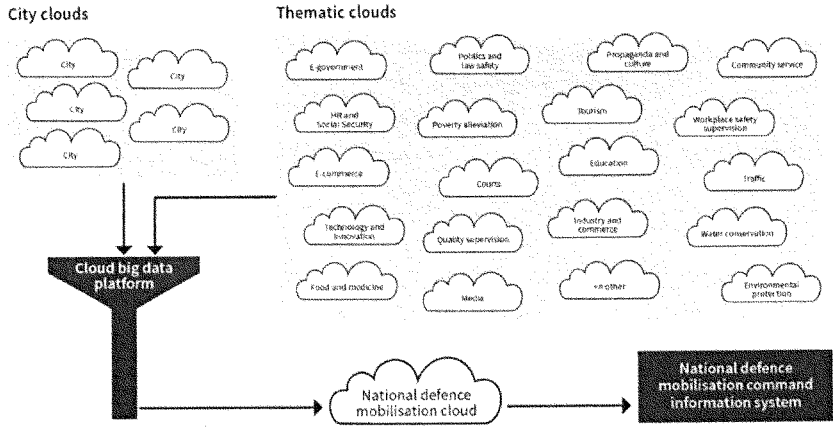

Figure 2 The concept of defence mobilisation and smart cities data integration and processing from Mapping China's Technology Giants: Supply chains and the global data collection ecosystem.

This is partly tied to administrative efficiency objectives set over two decades ago, before current technical capabilities existed. I noted in a 2018 article for *China Brief*[7] that in his report to the 15th Party Congress in 1997, then-CCP General Secretary Jiang Zemin noted that a bloated, inefficient bureaucracy hampers economic development, and the Party's ability to manage both itself and its relationship with society. His prescription was the establishment of a "highly efficient, well-coordinated and standardized administrative system."[8] Streamlining administration does more than improve the government's capacity to provide advertised administrative services, it improves the Party-state's overall visibility and, if effective, ability to predict and respond to problems (both "normal" governance problems and authoritarian control).

Current public conversation on China's capabilities among China analysts can often, misleadingly, focus on PRC discussion on its challenges with the integration and processing of data. Hundreds of companies' products are involved in smart cities projects across the PRC, making the implementation appear chaotic and uneven. Standardization is taking place at the design level, however, which indicates that seamless interoperability between smart cities systems is possible to achieve. While these capabilities are not currently at an optimal state, the trajectory appears to be in the Party-state's favor and levels of standardization across database schema for tools like Facial Recognition Systems improve. There is a constant evolution with digital technology. We must imagine technology's trajectory and future use cases to adequately develop policies governing their use. For now, the critical domains of influence are in possessing infrastructure, the storage, processing capacity and the data contained within it. If they invest the time and cost into doing so, the actor that controls those means can later control much more in terms of how technologies or the data derived from and passing through them are used.

In a report earlier this year for the National Endowment for Democracy, I highlighted how domestically, technologies are being researched and developed to meet the needs of the CCP, which are typically set out in government standards documents.[9] Government and research institutes collaborate with companies on national standards technical committees to standardize equipment development and the requirements that companies must meet to successfully bid for a project. For instance, a 2015 document GA/T1334 on the technical requirements for facial recognition in security systems was drafted through the cooperation of over a dozen bodies, including research institutes, such as the Chinese Academy of Sciences, the National University of Defense Technology, and the First Research Institute of the Ministry of Public Security; technology companies, such as Hikvision and Dahua; and public security bureaus, such as the Shanxi Provincial Public Security Department and the Wuhan Public Security Bureau. Documents like these are used as a basis for technical requirements in government procurement contracts.

In practice, local governments across the PRC have not yet achieved seamless interoperability between government departments and with other local governments using smart cities platforms, but this does not mean that it will remain out of reach. The setting of standards, and the requirement that project bidders meet those

standards, makes it more likely that plans such as Skynet or Sharp Eyes will gain cohesion and be successfully implemented, despite the many players involved. The same logic applies at the international level. Although the PRC cannot force its standards on other countries, it can help to set standards that become the global norm and ease the international adoption of its technology, effectively embedding the CCP's political values and increasing the regime's ability to exploit this advantage and project sharp power.

Recommendations for U.S. Policy

Recalibrate data security policy and privacy frameworks to account for the Chinese state's use of data to reinforce its political monopoly. Companies and governments too often assume that other governments' data and privacy regulations share the same goals as their own. That isn't true when it comes to the Chinese party-state and PRC-based companies, even if common vocabularies are used or if some policy drivers are similar. In the PRC, unlike in liberal democracies, data security and privacy concepts (including draft legislation) reinforce the party-state's monopoly power. Companies and governments need to recognize this risk and calibrate their policies to account for it.

Collaborate with like-minded countries to develop systems for improving risk-based approaches to improving the regulation of data transfers. Organizations must assess the value of their data, as well as the value of that data to any potential party in their supply chain that may have access to it or that might be granted access. In an age in which information warfare and disinformation campaigns occur across social media platforms and are among the greatest threats to social cohesion, data that's about public sentiment is as strategically valuable as data about more traditional military targets. Risk needs to be understood in a way that keeps up with the current threat landscape, in which otherwise innocuous data can be aggregated to carry meaning that can undermine a society or individuals.

Take a multidisciplinary approach to due diligence. Governments, businesses and other organizations need to develop frameworks for conducting supply-chain reviews that take into account country-specific policy drivers. Developing such a framework shouldn't be limited to just assessing a vendor's risk of exposure to political risk. It should also include detailed analysis of the downstream actors who have access to the vendor's data (and must include analysis of things such as the broader data ecosystem they're a part of and the obligations those vendors have to their own governments). Taking this more holistic approach to due diligence will better ensure that data can be protected in an effective way.

[Endnotes appear on the following page.]

Endnotes:

[1] Skynet Project (天网工程) refers to video monitoring equipment, mostly at major intersections, law and order checkpoints, and other public assembly locations. It uses GIS mapping, image gathering, transmission and other technology to improve real-time monitoring and information recording. Sharp Eyes Project (雪亮工程) is an extension of the Skynet project. In addition to surveillance cameras, Sharp Eyes is focused on building video image information exchange and sharing platforms and county–village–township comprehensive management centers. It is applied to efforts including state security, anti-terrorism, enhanced logistics, security supervision, and the prevention and control of criminal activity.

[2] Samantha Hoffman and Nathan Attrill, *Mapping China's Technology Giants: Supply chains and the global data collection ecosystem*, Australian Strategic Policy Institute (8 June 2021), https://www.aspi.org.au/report/mapping-chinas-tech-giants-supply-chains-and-global-data-collection-ecosystem.

[3] Samantha Hoffman, *Engineering global consent: The Chinese Communist Party's data-driven power expansion*, Australian Strategic Policy Institute (2019), https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2019-10/Engineering%20global%20consent%20V2.pdf?VersionId=eIvKpmwu2iVwZx4o1n8B5MAnncB75qbT.

[4] "7*24 小时实时监测," InsiderSoft, https://archive.vn/jJeJ0.

[5] ""梁浩宇：中译语通"全球公开大数据"助防安全风险" ", GTCOM, 2017, http://archive.is/FVJHM.

[6] Maya Wang, "China: Big Data Fuels Crackdown in Minority Region," (2018). https://www.hrw.org/news/2018/02/26/china-big-data-fuels-crackdown-minority-region.

[7] Samantha Hoffman, *Double-Edged Sword: China's Sharp Power Exploitation of Emerging Technologies*, National Endowment for Democracy (2021), https://www.ned.org/wp-content/uploads/2021/04/Double-Edged-Sword-Chinas-Sharp-Power-Exploitation-of-Emerging-Technologies-Hoffman-April-2021.pdf.

[8] Jiang Zemin, Hold High the Great Banner of Deng Xiaoping Theory for an All-round Advancement of the Cause of Building Socialism With Chinese Characteristics' Into the 21st Century: Report Delivered at the 15th National Congress of the Communist Party of China on September 12, 1997, (Beijing Review, 1997).

[9] Hoffman, *Double-Edged Sword: China's Sharp Power Exploitation of Emerging Technologies*.

PREPARED STATEMENT OF YAQUI WANG

Chairman Merkley, Chairman McGovern, distinguished members of the Commission, thank you for the opportunity to speak on this issue dear to my heart. I owe my presence here today to the relative internet freedom China once had, and to the respect for freedom of information in the United States.

I was born and grew up in China. As a teenager, every day I would go online and listen to Voice of America's "Special English," a news program broadcast in slow-speed English. That's how I started to learn English, and that's also how I and many others in China got information uncensored by the Chinese government.

That was 15 years ago, and Beijing has since gotten so much better at controlling the internet. It's not only that many foreign websites have been blocked, but also that some people from China who now live in the U.S.—with free internet readily accessible—still go back to the censored Chinese internet to get their news.

I'd like to use my five minutes to focus on WeChat and TikTok, two Chinese apps that have a significant presence in the U.S.

First and foremost, it is essential to remember that all Chinese companies are subject to the control of the ruling Chinese Communist Party (CCP).

The Chinese diaspora heavily relies on the super-app WeChat for information, communication, and even political organizing. This allows Beijing to shape the Chinese diaspora's views in ways more amenable to the CCP. It allows Beijing to know a lot about the people who have left China, down to things like who is meeting whom, at what time, and where. And it also allows Beijing to surveil and potentially influence and mobilize an important demographic in the U.S.

Earlier this year, a network of fake social media accounts linked to the Chinese government attempted, but failed, to draw Americans out to real-world protests against racial injustice. The reason we know about the scheme is because it happened on Facebook, YouTube, and Twitter—American companies that periodically disclose influence operations, including by government and government-aligned actors. We don't know whether similar manipulations are also happening on WeChat because it's difficult to do research.

Then there is TikTok, which has far deeper reach into the lives of the American public, especially young people. One thing lawmakers need to understand is that the company's algorithm largely decides what users see. There is no way for outsiders

to know what information is being suppressed or promoted on TikTok because of government influence. The Australian Strategic Policy Institute's analysis of the hashtag #Xinjiang showed a depiction of the region that glosses over the human rights suffering and instead provides a version that is filled with smiling and dancing Uyghurs.

In short, there is a lot we don't know about what Chinese tech companies are doing in the U.S.—what is being censored, promoted, and suppressed, and how data is being harvested, accessed, used, and shared. There are risks that these companies can be or are being used by the Chinese government to undermine the rights of American users.

Congress has recently increased its scrutiny of American tech companies. Chinese tech companies' rising popularity in the U.S. and their ties to the Chinese government should give added urgency to efforts to pass laws to require tech companies—regardless of where they are headquartered—to protect user data and to be more transparent in how they moderate content.

Lastly, here I speak not as an expert, but as a member of the Chinese immigrant community in America: to counter harm from Chinese tech companies and improve independent, professional Chinese-language media, the U.S. Government should invest in journalism training and similar programs for aspiring Chinese-language journalists. Making fact-based information available in our native language is one of the most effective ways to counter Beijing's malign influence.

Thank you and I look forward to your questions.

RECOMMENDATIONS FOR THE U.S. GOVERNMENT

1. Enact comprehensive data protection laws that require all tech companies to practice data minimization for all users; conduct human rights impact assessments that address all aspects of companies' operations, including their underlying business model; and require human rights due diligence for their operations globally.
2. Consider regulations that encourage transparency from all social media platforms, including disclosure of their content moderation policies and enforcement, such as what content they've censored or suppressed because of their own policies or at the request of governments.
3. Improve independent, professional Chinese-language journalism by investing in journalism training and similar programs, expanding the space for Chinese-language speakers to learn about and discuss human rights issues inside China and around the world.
4. Invest in open-source technologies that provide other channels of communication and enable people in China to more easily circumvent censorship.

WECHAT CENSORSHIP AND SURVEILLANCE AFFECTING THE CHINESE DIASPORA

International WeChat users are estimated at between 100 million and 200 million; there are an average of 19 million daily active users in the United States.

Over the past couple of years, I've interviewed members of the Chinese diaspora around the world on the Chinese government's activities undermining human rights abroad. A recurring problem I've run into is that some of my sources only wanted to use WeChat to communicate, mainly because they had not installed any other messaging apps.

The centrality of WeChat in information acquisition and communication among the Chinese diaspora, especially first-generation immigrants from China, should be a source of real concern.

Chinese law requires internet companies to store internet logs and relevant data for at least six months to assist law enforcement. WeChat's own privacy policy notes that it may need to "retain, disclose and use" user information in response to requests from the government. Hence, the Chinese government can—if it wants—know a lot about the people who have left China, down to things like who is meeting whom, at what time, and where. And because WeChat is a payment app as well, it can see to whom they send money or from whom they get it or even who pays for dinner.

WeChat is also where many members of the Chinese diaspora obtain information, including about the countries they immigrated to. A survey of Mandarin speakers in Australia found that 60 percent of those polled identified WeChat as their primary source of news and information, while only 23 percent said they regularly accessed news from mainstream Australian media, such as the Australian Broadcasting Corporation and the *Sydney Morning Herald*.

Some of the most popular publications catering to the diaspora originated on WeChat. In order to attract readership, traditional Chinese-language media outlets now also publish through WeChat. In this sense, news produced by a local Chinese-

language outlet in New York goes through censors in Beijing before it reaches the Chinese-speaking community in New York.

Because of the importance of WeChat among the Chinese diaspora, some political parties and politicians in countries such as Australia, Canada, and the U.S. have opened their own WeChat accounts or regularly utilize popular accounts to reach out to their Chinese speaking constituencies.

And there is evidence that the Chinese government, through censorship on WeChat, has interfered with communications between elected officials and constituents in Western democracies.

In September 2017, Jenny Kwan, a member of the Canadian parliament, made a statement regarding the Umbrella Movement in Hong Kong in which she praised the young protesters who "stood up and fought for what they believe in, and for the betterment of their society."

The statement and anything related quickly disappeared.

After it was taken down, Kwan told me in an email, "We posted the statement on Sept 6, 2017. One hundred people viewed it, 1 like and 3 comments were posted before it was deleted by the WeChat management. We only noticed that it was taken down since you asked the question."

In this case, the Chinese government quietly and effortlessly prevented an elected official in a democracy from being heard by her own constituents. Imagine the consequences if the Chinese government decided to disrupt these conversations on a broader scale.

CENSORSHIP ON TIKTOK

TikTok has repeatedly stated that the Chinese government has not asked it to remove any content, and that if it does, the company will not comply. But such reassurances have not found broader acceptance.

For example, there are few videos on TikTok concerning the Hong Kong protests—even though the largely youth-led movement has garnered massive international attention. After American teenager Feroza Aziz posted a video condemning the Chinese government's mass detention of Uyghur Muslims that went viral, her account was suspended. TikTok asserted the suspension was the result of an earlier satirical video of hers referencing Osama Bin Laden being mistakenly flagged for violating the app's anti-terrorism policy.

In 2020, my colleague and I tried to test some of these concerns. We started by uploading clips of Tank Man, the young man who famously stood his ground in front of a procession of Chinese army tanks during the 1989 Tiananmen Square crackdown in Beijing.

One clip, uploaded to an account registered in Australia, was visible to the account holder but not to anyone else. When we raised the issue with TikTok, representatives of the company said via email that the video was "incorrectly partially restricted based on guidelines related to displaying identifiable military information." Our video was later reinstated.

After I published an article mentioning the incident, including TikTok's response, Tik Tok's representative emailed me, calling my reporting "misleading" and demanding retraction. Because we considered our report to be fair and accurate, we declined to do so. Yet, I was taken aback by the incident and thought about how I would have acted differently if I were an independent researcher without the support of an institution—it's possible I would have given in to this pressure.

PREPARED STATEMENT OF JONATHAN E. HILLMAN

Chairman Merkley, Chairman McGovern, and distinguished Members of the Commission, thank you for holding this important hearing and asking me to participate.

This testimony draws from my book, *The Digital Silk Road: China's Quest to Wire the World and Win the Future*, and related research at the Center for Strategic and International Studies, where I direct the Reconnecting Asia Project.[1]

The bottom line is that China is gaining globally through its Digital Silk Road and positioning itself to reap commercial and strategic rewards, but its dominance is far from assured. The United States has several advantages, including world-leading research universities, innovative companies, deep pools of private capital, openness to immigrants, and a global network of partners and allies. The question is whether the United States can rise to the challenge and lead a coalition that offers real benefits to the developing world. In much of the world, cost trumps security. Competing will require expanding the availability of affordable alternatives.

If uncontested, China's Digital Silk Road will undermine U.S. economic and strategic interests. Developing economies will rise in the coming decades, as under-

scored by demographic trends, and offer vast opportunities for growth.[2] For example, Nigeria, the world's twenty-eighth largest economy in 2017, is projected to become the world's ninth largest economy by 2100. During the same period, India will move from seventh to third place. These projections provide a glimpse of an emerging world that the United States can engage with, and benefit U.S. workers and companies, or allow China to cement a position of strength.

China also stands to gain intelligence and coercive powers if it achieves its global network ambitions. It could have eyes and ears not merely walking around foreign capitals but woven into foreign government buildings, public security command posts, and data centers. It could learn about scientific breakthroughs as they are made, corporate mergers and acquisitions as they are contemplated, and patents before they are filed. On "the worst possible day," Beijing could disrupt, disable, or destroy its adversaries' communications, financial markets, and military systems.[3]

These risks must be taken seriously because the warning signs are already here. For five years, servers at the African Union headquarters sent data to Beijing covertly in the dead of night. Cameras watching over Pakistani streets came equipped with hidden hardware while others malfunctioned. A Chinese subsea cable that stretches from Africa to South America added little but debt to Cameroon's economy. Laos's first satellite is actually majority-owned by Beijing. These are the signs of digital dependency.

The testimony that follows describes how we got here, provides a tour of the battlefield, and outlines what the United States needs to do. First, it explains how U.S. mistakes paved the way for China's telecommunications giants. Second, it provides an overview of the global digital infrastructure competition in four areas: wireless networks, smart cities, internet backbone, and satellites. Third, it explains why a coalition is necessary to compete, identifies partners, and notes areas of friction that must be managed. Finally, it summarizes recommendations for U.S. policy.

I. Learning from Past Mistakes

The Digital Silk Road sits at the intersection of Chinese leader Xi Jinping's signature policy efforts. It is the technology dimension of China's Belt and Road Initiative, Xi's vision for moving China closer to the center of everything through infrastructure projects, trade deals, people-to-people ties, and policy coordination. By helping Chinese tech companies expand into foreign markets, it also advances "Made in China 2025," which aims to capture dominant market shares in high-tech industries.

The Digital Silk Road was first mentioned in 2015, as the "Information Silk Road," but its roots run much further back. During the 1980s and 1990s, Chinese leaders fashioned industrial policies and negotiated deals with foreign companies that helped Chinese telecommunications firms dramatically improve their capabilities. Through the Digital Silk Road, China aims to further reduce its dependency on foreign companies while making more of the world dependent on Chinese technology.

Conventional narratives usually overlook or oversimplify this longer history. The story often told in Washington is that Huawei and other Chinese firms essentially lied, cheated, and stole their way to success. To be sure, there was plenty of unfair and illegal behavior, from receiving massive state support to blatantly copying competitors' products. But this oversimplified narrative is dangerously self-serving. It avoids taking responsibility, misses mistakes, and offers little insight for competing more effectively. An honest assessment leads to three hard truths:

1. **U.S. leaders overhyped the benefits of connectivity.** Triumphant in the aftermath of the Cold War, U.S. commentators predicted that the Chinese Communist Party (CCP) was digging its own grave by adopting satellite TV, the internet, and other communications systems at home. But CCP leaders set out to modify and wield these tools for their own purposes. Today, commentators warn that China is exporting authoritarianism. In reality, telecommunications systems are tools, neither inherently good nor bad. Understanding impacts, and fashioning solutions, requires looking closely at local contexts.

2. **Foreign companies rushed into China and helped to create their own competitors.** Foreign manufacturers handed over access to their knowledge and capabilities, consultants helped transform Chinese companies' business operations, and researchers went to work for their former companies' competitors. After China's domestic telecommunications capabilities matured, Chinese officials restricted market access for foreign companies. Avoiding these mistakes in emerging technologies

will require closer public-private cooperation among the United States, its partners, and allies.

3. **Chinese companies expanded into overlooked markets.** U.S. companies focused primarily on larger, wealthier markets, leaving Chinese providers to serve lower-income and rural markets. Even as Chinese tech companies now face greater scrutiny in advanced economies, they are still building a position of strength in emerging markets, where most of the world's population growth is expected. To compete in those markets, the United States and its partners have to offer affordable alternatives.

II. Navigating the Battlefield

China's Digital Silk Road is advancing in four key areas: wireless networks, smart cities, internet backbone, and satellites. While not exhaustive of China's digital activities, these activities literally stretch from the ocean floor to outer space, and they enable artificial intelligence (AI), big data applications, and other strategic technologies. In all four areas, China is gaining globally and positioning itself to reap commercial and strategic rewards, but its dominance is far from assured. It also has vulnerabilities and weaknesses that the United States and its allies could exploit.

Wireless Networks

The world is beginning to splinter between countries that use Chinese suppliers for their wireless networks and those that do not. The latter category is primarily wealthy democracies. Most NATO member states have raised barriers to Huawei's participation in their 5G rollouts. Australia and Japan have imposed restrictions as well. India has not made a final judgement, but it did not include any Chinese suppliers in its initial 5G trials.

In most of the developing world, however, Chinese providers are moving ahead. They are often the incumbent providers in these markets, having won significant market share after offering equipment at prices 20–30 percent below their competitors. For example, Huawei is believed to have supplied roughly 70 percent of Africa's 4G networks. 5G networks are often built on top of existing networks, and the cost of starting over may appear prohibitive for lower-income countries.

Open Radio Access Networks (Open RAN) could tilt the playing field in favor of the United States. By virtualizing parts of the network that are currently served by proprietary hardware, Open RAN allows operators to mix and match different network components from different vendors. For operators, the potential upside is greater vendor choice, lower deployment costs, and less risk of being locked into a single vendor. The United States stands to benefit because its companies are leading providers of the specialized software and semiconductors that Open RAN relies upon.

Open RAN could take anywhere from several years to a decade to mature. There are already promising examples of Open RAN being deployed around the world, at all speeds, from 2G to 5G. But the flip side of greater vendor choice is greater complexity. There are still kinks to work out as networks combine components from different suppliers. Smaller operators may not have the necessary technical expertise, while larger operators may not have the patience. Some may still prefer the ease of going with a single vendor, even if it is more expensive.

But the 5G race is just getting started. A third of the world's population lives in countries where 1GB mobile broadband plans are unaffordable for average earners. Among those with mobile connections, only 15 percent of users are expected to use 5G by 2025, while nearly 60 percent of mobile users will rely on 4G. The global market is still up for grabs, and the United States can establish a position of strength by making targeted investments at home and expanding financing and training activities abroad, as outlined below in Part IV.

Smart Cities

Megatrends in innovation and urbanization are turning cities into ground-zero for competing approaches to development and governance.[4] The arrival of faster networks, cheaper sensors, and more sophisticated analytics promises to help reduce crime, ease traffic, and improve other public services, while also impacting civil liberties, data security, and other public concerns. By 2030, seven out of ten people in the world will live in cities, with urban populations growing fastest in Africa and Asia. Around the world, planners will need to decide which systems and safeguards to adopt.

China's "safe city" model, which emphasizes security applications such as surveillance cameras, is gaining traction. Only China has companies that are competitive

at every step of the surveillance process, from manufacturing cameras to training AI to deploying the analytics. At home, Chinese companies never question the government's use of these capabilities, and government subsidies fuel their global expansion. Hikvision and Huawei are China's leading providers globally, followed by Dahua and ZTE. Altogether, Chinese firms have exported smart city products and services to more than 100 countries.[5]

These firms offer attractive capabilities at cut-rate prices. Using their "safe city" systems, they claim, will reduce crime, increase economic growth, and even help fight the Covid-19 pandemic. Facial recognition and behavior analysis identifies wanted criminals and alerts the police to unusual behavior, such as wandering near restricted areas. Measuring traffic flows and enforcing driving laws improves congestion. Temperature-sensing cameras identify people with fevers. These and other capabilities can be fed into a central database and command center. Offers that come with financing can give the impression that these systems will essentially pay for themselves.

But China's "safe city" exports are also vulnerable in several respects. Cases in Kenya, Pakistan, and elsewhere show crime rising, cameras malfunctioning, and other challenges.[6] Greater transparency and accountability would surely unearth more instances of overpromising and underdelivering. Chinese firms have also been willing to sell to essentially anyone, creating reputational risks. Over time, companies that press forward without safeguards may find their clientele shrinking to a list of names they would not care to advertise.

These missteps open the door for the United States and its allies to provide alternatives. For example, they could offer a "Sustainable City" certification with financial support that emphasizes commercial viability, energy efficiency, social safeguards, and data security. This is another area where U.S. domestic renewal and global competitiveness are strongly aligned. More cutting-edge examples of smart cities at home—such as Charlotte, Las Vegas, and Pittsburgh—will position U.S. companies to succeed abroad.

Internet Backbone

China is redrawing the internet as it builds key connections and nodes, especially subsea cables and data centers, beyond its borders. Its biggest moves are happening in Asia, Africa, and Latin America, where Chinese tech companies face less scrutiny and demand for digital infrastructure is expected to grow significantly in the coming years. Africa, for example, is home to 17 percent of the world's population but less than 1 percent of the world's installed data center capacity. If China's asymmetric strategy for global data flows is successful, its firms will carry, store, and mine more of the world's data while its domestic networks will move further out of foreign reach.

In just a decade, China has graduated from being dependent on foreign companies for subsea cables, which carry over 95 percent of the world's international data, to controlling the world's fourth major provider of these systems. Before being sold to Hengtong Group in 2020, Huawei Marine (a joint venture between Huawei and Global Marine, a UK firm) laid enough cable to circle the earth, including transcontinental links from Asia to Africa and from Africa to South America. These connections avoid U.S. and allied territory and could become even more valuable during a conflict.

China's cloud providers are also marching into emerging markets. The leading U.S. cloud providers—Amazon, Microsoft, and Google—have a massive first-mover advantage. But the Chinese government is following a familiar playbook: pushing data localization rules that favor its providers, leveraging state financing, and packaging services with hard infrastructure. Foreign governments and businesses may find it difficult to switch providers down the road. On top of the normal expenses of migrating from one cloud to another, they may also face Chinese economic coercion.

Meanwhile, the Chinese government is tightening its control over networks at home. Like a medieval castle, China's domestic network forces international connections into a handful of chokepoints and requires foreign carriers to use one of China's "Big Three" state-owned telecom firms (China Telecom, China Mobile, and China Unicom). This architecture gives Beijing an unrivaled ability to monitor, censor, and cut off traffic. Wealthier and more technically savvy individuals can find ways to access the global internet, although popular tools such as virtual private networks (VPNs) have been heavily curtailed.

But China's asymmetric strategy also comes with costs. Restricting access to the global internet harms the ability of Chinese firms to innovate, and restricting international connections leaves even China's Big Three dependent upon foreign carriers for international data transit. Roughly 80 percent of China's international traffic

passes through U.S. and European carriers.[7] Mainland Chinese cities are absent among the rankings of the world's most connected hubs, which all have open internet exchanges, a model that remains anathema to Party leaders. The CCP's conundrum is that greater international connectivity requires giving up some control.

The United States and its allies have several enduring advantages in this domain. The United States remains the world's leading hub for internet traffic, a position made possible by its open approach to data flows, innovative companies, and attractive market. The top three subsea cable providers are based in the U.S., Europe, and Japan and are responsible for nearly 90 percent of the global market. Three U.S. companies control over half of the global market for cloud services, and the quality of their offerings is consistently ranked higher than their Chinese competitors. Maintaining these advantages, however, will require competing in tomorrow's markets.

Satellites

China has gone from latecomer to leading provider of satellite services, especially for developing markets. Following major events in the 1990s, particularly the Gulf War and the 1996 Taiwan Strait Crisis, China set out to develop its own global navigation satellite system. Completed in 2020, China's BeiDou system is more accurate than the Global Positioning System (GPS) in the Asia-Pacific region, although slightly less accurate globally, and its satellites occupy fewer orbital planes, making maintenance easier. The system also allows users to send short text messages, and its larger footprint increases its availability. In 165 capital cities, BeiDou provides more extensive coverage than GPS.[8]

BeiDou advances both China's commercial and military interests. When China exports electronics, increasingly it is exporting the BeiDou system, which is included in phones, vehicles, farm equipment, and consumer products. In 2019, China's satellite navigation sector pulled in $64 billion, and by 2029, the global market for satellite navigation devices is projected to grow to about $360 billion. BeiDou includes even more powerful services that guide Chinese missiles, fighter jets, and naval vessels. China has begun offering these military-grade services to partners and could use them as a sweetener in the future when selling arms. Strategically, China is reducing its reliance on GPS and increasing its partners' reliance on BeiDou.

China is also carving out a niche as the go-to provider for developing countries that want their own communications satellites. For about $250 million, only a fraction of which is required up front due to Chinese state financing, countries can acquire their own geostationary communications satellite. China also provides ground stations, testing, training, launch, and operations support. As of early 2021, at least nine countries have bought or are in the process of buying communications satellites from China. Several satellites have experienced launch or operational challenges, and many of China's customers have struggled financially.

Low-earth orbit (LEO), between 500 and 2,000 kilometers high, is the next frontier for competition. LEO broadband constellations could expand access to low-latency, high-speed internet globally. In addition to reaping commercial rewards, nations with leading LEO broadband providers could enjoy increased resiliency in their communications, accuracy in positioning services, and enhanced early warning capabilities. A small group of primarily U.S. and European companies, including SpaceX, Amazon, and OneWeb, are on the cutting edge of these efforts.

Some are using intersatellite-laser links, which allow satellites to exchange data without passing through a ground-based intermediary, increasing performance and complicating government attempts to monitor communications.

China has its own LEO plans. Its companies are behind in the race to launch LEO constellations, but they have generous state support, making profitability less of an immediate concern. This second-mover, state-led strategy allows China to see what works and emulate foreign successes. Some countries may prefer China's alternative, which will surely favor state control of communications. If the LEO competition turns into a marathon, Beijing could also leverage its lending along the Belt and Road to obtain landing rights and obstruct competing efforts.

If the United States seizes this opportunity, the coming wave of LEO constellations could undercut China's advantage in overlooked markets. Western LEO broadband providers could serve rural and less-wealthy markets without building all the ground infrastructure that has deterred them in the past. Some financial assistance—from U.S. and allied governments, multilateral development banks, or even philanthropists—will be required to make these services affordable in low-income markets. Commercial diplomacy, outlined in Part IV, could help U.S. providers secure landing rights.

III. Leading a Coalition

China presents a challenge of scale. Its population of 1.4 billion provides Chinese companies with preferred access to the world's largest market of middle-class consumers and the government with access to an ocean of data. The Chinese government's ability to direct resources, even if inefficient and wasteful, is giving a boost to emerging technologies and subsidizing the cost of Chinese equipment globally.

Meeting this challenge will require the United States to lead a coalition. In the absence of a coalition, China can pit companies against each other to access their technology, just as it did during the 1980s and 1990s, when U.S. and allied telecom companies undercut each other in their race to access China's market. Without the commercial incentives that a coalition could offer, U.S. and allied companies are likely to remain focused on the largest, wealthiest markets, overlooking the developing world.

A group of wealthy democracies with strong common interests could provide a critical mass. Collectively, seven U.S. allies—Australia, Canada, France, Germany, Japan, South Korea, and the United Kingdom—outspend China on R&D. Although the pandemic has clouded their economic prospects, they are still projected to account for roughly a fifth of global GDP in 2030. All these countries are U.S. treaty allies and democracies, but the coalition's mission must extend beyond simply protecting wealthy democracies. It must also engage and support rising hubs on the periphery, large economies in the developing world with a mixture of overlapping and distinct interests.

Two bridges are especially critical to building this coalition. The first bridge stretches across the Atlantic. Despite common values, the United States and Europe look at global networks differently. Lacking a technology champion of similar size, some European leaders view U.S. technology companies as even more threatening than Chinese companies. The European Union is trying to position itself as a middle option between the open U.S. model and the state-centric Chinese model. Disagreements over data flows and content regulation must be managed through existing mechanisms and new avenues such as the EU-U.S. Trade and Technology Council.

There are real prospects for stronger transatlantic cooperation as well. The United States could remove obstacles to cooperation by adopting national data privacy regulations aligned with the EU's own General Data Protection Regulation, encouraging greater competition in the digital economy, and implementing the OECD global minimum tax agreement. At the International Telecommunication Union, a UN agency, the United States and its European allies should work to elect Doreen Bogdan-Martin as the next director-general and advance socially responsible standards in emerging areas such as AI surveillance, while blocking Chinese proposals to hand governments more control over the internet.

The second bridge extends into the developing world and begins with India, which is expected to become the world's most populous country in the coming years, making it the critical swing state in the global network competition. Realizing India's promise as a growing market and hub for digital services and manufacturing will require breaking its dependency on Chinese hardware.

In 2019, India imported about 40 percent of its telecommunications equipment from China and nearly two-thirds of its data center equipment from China and Hong Kong. Three of India's four largest carriers rely on Huawei and ZTE equipment for 30–40 percent of their networks.

Ultimately, India's participation in the coalition should be based on actions, not aspirations. New Delhi is the world's leader in internet shutdowns and has declined to join talks on e-commerce at the World Trade Organization and data flow initiatives at the G20. The coalition should work with India to craft a roadmap for addressing these shortcomings. India's reforms could be incentivized with policies that strengthen its manufacturing sector, diversify supply chains, connect its own citizens, and win customers in foreign markets.

IV. Recommendations

A successful strategy for meeting this global challenge begins at home, but it does not end there. The United States still has its own communities to connect and a digital divide that will widen if left to market forces. It must push forward the frontiers of technology by educating and attracting the next generation of innovators, ensuring they have the resources to succeed and the competitive space for new businesses to flourish. It must fashion data policies that protect citizens' privacy and their security. At the same time, the United States must compete in tomorrow's markets. With that international competition in mind, the recommendations below focus on sharpening U.S. tools, expanding affordable alternatives, and exploiting China's weaknesses.

Sharpen U.S. Tools

1. **Unleash the U.S. International Development Finance Corporation (DFC).** Update budget rules to allow the DFC to make better use of its equity authority, create a position at the DFC for a senior official in charge of ICT investments, and increase the share of digital infrastructure projects in the DFC's portfolio.

2. **Expand the U.S. Commercial Foreign Service** to remove and prevent barriers to U.S. suppliers in key emerging markets. In Africa, for example, China has 10 to 40 government representatives for every U.S. foreign commercial service officer there. This expansion should include a focus on recruiting individuals with technology backgrounds.

3. **Conduct a global networks assessment.** The National Intelligence Council, with input from U.S. agencies and the private sector, should assess key trends and scenarios for telecommunications networks and their implications for U.S. interests over the next decade. An unclassified version of the assessment should be made public.

4. **Update defense commitments to include a greater focus on technology.** The recent AUKUS partnership, which includes a technology sharing dimension, is an encouraging example of updating defense partnerships for the digital age. More should be done to adopt existing tech and invest in future capabilities. For example, NATO members could be permitted to count some spending on critical digital infrastructure with a direct application to NATO communications, such as select 5G systems, toward their overall spending obligations.[9]

Expand Affordable Alternatives

5. **Launch digital pilot projects.** As the U.S. and its allies look to launch pilot projects for the G7's Build Back Better World partnership and related efforts, such as the Blue Dot Network, they should put an emphasis on digital infrastructure projects, which in addition to being important, often cost less and take less time to complete than large transport and energy projects.

6. **Put a price on security.** Provide technical assistance to improve how countries assess costs and reach decisions. The initial price tag on Chinese projects often only includes the up-front costs associated with construction, overlooking maintenance and operations costs. Rather than simply warning against security risks, the economic costs of those risks should be estimated, widely advertised, and factored into cost-benefit analyses.

7. **Pursue a digital trade deal** that pushes back against the rise in data localization policies, supports the responsible use of ICT and emerging technologies such as AI, and lowers barriers to access for small businesses.

8. **Develop a "Sustainable Cities" certification** for cities and companies that emphasizes commercial viability, energy efficiency, social safeguards, and data security. Cities receiving the certification could receive financial and technical assistance. Companies that qualify could receive priority when competing for projects in those cities.

9. **Create an Open RAN international academy.** Open RAN offers more choice and presents less risk of becoming locked into a single vendor, but it also adds complexity. This effort would train foreign operators and share specifications for tested and trusted combinations of hardware to reduce uncertainty.

10. **Launch a global cloud public-private partnership.** Work with U.S. companies and NGOs to support pilot cloud projects in emerging markets that package services, hard infrastructure, and training opportunities. In addition to building partners' technical capacities and increasing the adoption of trusted services, these projects could be used to incentivize openness to data flows.

11. **Bring LEO broadband to low-income markets.** Help U.S. LEO broadband providers secure landing rights overseas, and work through multilateral development banks to provide financial support for customers in low-income markets to access these services.

Exploit China's Weaknesses

12. **Invest in technologies that challenge authoritarian networks.** Increase funding for the Open Technology Fund (OTF) and other efforts to support tools such as Tor and Signal that help dissidents communicate securely and reconstitute their websites after an attack. More sophisticated tools will also make China's authoritarian approach more expensive to maintain.

13. **Expose false claims.** Chinese companies have left a trail of exaggerations and outright lies about their "safe city" systems, surveillance cameras, data centers, and other products. Technical assistance and public-awareness campaigns that un-

cover and expose these shortcomings—not just security flaws but also performance shortcomings and broken promises—could help shift the cost-benefit analysis of decisionmakers.

14. **Expand information-sharing.** Much of China's commercial diplomacy is conducted bilaterally and opaquely, which maximizes its negotiating power, limits outside scrutiny, and prevents its partners from sharing information with each other. The United States should encourage countries to adopt laws that require publishing government contracts and create opportunities for developing countries to share information and lessons learned with each other.

15. **Cement first-mover advantages.** China is attempting to match and surpass U.S. digital capabilities, but it remains behind in cloud computing, LEO broadband, and other important areas. Even as U.S. policymakers address areas where the United States lags (e.g., 5G), they must help U.S. workers and companies press these existing advantages through policies that support innovating, expanding into foreign markets, and striking long-term partnership agreements.

Endnotes:

[1] Jonathan E. Hillman, *The Digital Silk Road: China's Quest to Wire the World and Win the Future* (New York: Harper Business, 2021); Jonathan E. Hillman, *The Emperor's New Road: China and the Project of the Century* (New Haven: Yale University Press, 2020); "Reconnecting Asia Project," Center for Strategic and International Studies, Accessed November 12, 2020, https://reconasia.csis.org.

[2] Gulrez Azhar, et al. "Fertility, morality, migration, and population scenarios for 195 countries and territories from 2017 to 2100: a forecasting analysis for the Global Burden of Disease Study." *The Lancet*, 396, no. 10258 (2020). Doi: https://doi.org/10.1016/S0140-6736(20)30677-2.

[3] Thomas Donahue, "The Worst Possible Day: U.S. Telecommunications and Huawei," *Prism 8*, no. 3, https://ndupress.ndu.edu/Portals/68/Documents/prism/prism 8-3/prism 8-3 Donahue 14-35.pdf.

[4] Jonathan E. Hillman and Laura Rivas, "Global Networks 2030," Center for Strategic and International Studies, March 29, 2021, https://www.csis.org/analysis/global-networks-2030-developing-economies-and-emerging-technologies.

[5] Katherine Atha et al., "China's Smart Cities Development," SOS International, January 2020, https://www.uscc.gov/sites/default/files/China_Smart_Cities_Development.pdf.

[6] Sheridan Prasso, "Huawei's Claims That It Makes Cities Safer Mostly Look Like Hype," Bloomberg, November 12, 2019, https://www.bloomberg.com/news/articles/2019-11-12/huawei-s-surveillance-network-claims-face-

[7] Dave Allen, "Analysis by Oracle Internet Intelligence Highlights China's Unique approach to Connecting to the Global Internet," Oracle, July 19, 2019, https://web.archive.org/web/20210512021539/https://blogs.oracle.com/internetintelligence/analysis-by-oracle-internet-intelligence-highlights-china%E2%80%99s-unique-approach-to-connecting-to-the-global-internet.

[8] Toru Shima, "In 165 Countries, China's Beidou eclipses American GPS," Nikkei Asia, November 25, 2020, https://asia.nikkei.com/Spotlight/Century-of-Data/In-165-countries-China-s-Beidou-eclipses-American-GPS.

[9] Terry Schultz, interview with Simon Handler and Safa Edwards, NATO 20/2020 Atlantic Council, podcast audio, February 10, 2021, https://www.atlanticcouncil.org/ content-series/nato20-2020/ supersize-cyber-nato-20-2020-podcast/; Lindsey Gorman, "NATO Should Count Spending on Secure 5G Towards Its 2% Goals," Defense One, December 3, 2019, https://www.defenseone.com/ideas/2019/12/ nato-should-count-secure-5g-spending-towards-its-2-goals/161648/.

PREPARED STATEMENT OF HON. JEFF MERKLEY

Good morning. Today's hearing of the Congressional-Executive Commission on China on "Techno-Authoritarianism: Platform for Repression in China and Abroad" will come to order.

This hearing will explore China's role in embracing technology-enhanced authoritarianism and promoting its spread around the world. In China and around the globe, we are seeing that the same technology that drives the global economy, facilitates communication, enables financial flows, and provides the conveniences of modern life can also be used for repression. Without proper guardrails to protect privacy and basic human rights, technology can control populations, trample freedom of expression, and undermine institutions of democratic governance.

For the Chinese government and Chinese Communist Party, it starts at home. Over many years, the Commission has documented the development of what has become the most pervasive surveillance state the world has ever seen. Authorities embrace technologies such as artificial intelligence, blockchain, and cloud computing—the building blocks of the modern economy—to impose political and social control of targeted populations. These technologies offer the government an unprecedented degree of control, enabled by the collection of massive amounts of data from cell phones, personal computers, DNA, security cameras, and more.

Nowhere do we see this more tragically than in the Xinjiang Uyghur Autonomous Region. Today we will hear testimony outlining the extent of the surveillance in

Xinjiang, as well as the heart-wrenching toll on individuals and their communities. We will also hear from expert witnesses who will shed light on the use of technology in mainland China and abroad, both for legitimate purposes of government efficiency and digital connectivity but also to spread the web of repressive control to cities across China, regions across China, the developing world, and even the Chinese diaspora community in the United States.

This adds up to a complex picture. The technologies we will hear about have dual-use potential to be used for good or for ill. Many countries to which China exports surveillance systems and elements of the so-called "safe cities" model embrace these technologies out of a desire to combat crime or reduce traffic or provide municipal services. Yet these technologies, this high-tech authoritarianism, can be used to strip rights and dignity from millions of people across the planet.

Acting to defend freedom and to defend democracy will require the establishment of norms for the proper use and boundaries of this technology, but we can't stop there. We have to work with defenders of freedom across the globe to develop attractive and affordable alternatives.

This won't be easy. That's why Co-chair McGovern and I have convened this hearing. We need to hear from experts on how Congress, the United States Government, and the international community can address these difficult challenges. Just as the United States confronts limitations in its ability to shape the behavior of the Chinese government, so too will we face limitations in shaping the rest of the world, especially when it comes to technology that empowers everyday life. That's why we need smart action in concert with a coalition of partners.

I look forward to the testimony today to help us work to identify the approaches that can harness technology in a way that respects rather than endangers fundamental human rights.

PREPARED STATEMENT OF HON. JAMES P. MCGOVERN

Thank you, Mr. Chairman, for convening this hearing on the Chinese government's use of technology and digital platforms to expand and export its repressive policies.

Where there was once optimism that the internet and new technologies would create a more open, democratized global commons, there is now a cloud of darkness. Anti-democratic and authoritarian governments have learned to harness such technology as a means to assert social control.

This is no longer just about human rights abuses suffered by people over there. It is about the risks we now face from the phones in our pockets.

Take TikTok. It is immensely popular in the United States and can be a lot of fun, or so my kids tell me. It was developed by a Chinese company. There is nothing inherently wrong with that. But we hear reports that videos on topics sensitive to its government are blocked or disappear. Americans deserve to know whether China's censorship regime is intruding on their daily lives.

This concern is why the Commission, under my chairmanship in the last Congress, expanded its reporting to include "Human Rights Violations in the United States and Globally."

Our soon-to-be-released annual report will document how the Chinese government silences criticism, chills the expression of political views, and undermines international norms. The Commission's next hearing will look at the economic coercion aspect of this trend.

We cannot forget that the Chinese government's techno-authoritarianism is felt most gravely by the Uyghurs and other Turkic Muslims. The surveillance regime they have set up in Xinjiang is the most advanced and enveloping in the world. Is this the model for the rest of China and the world? This is the key question we hope today's witnesses will address.

How can the United States ensure that its exports do not abet the spread of the surveillance state? Can we harness international partners? How do individuals make sound consumer choices?

We are addressing an immensely complicated and technical set of issues. I'm pleased that our witnesses bring a breadth of expertise to these evolving challenges. I hope you will continue to share your research with us.

United States House of Representatives
Congressional-Executive Commission on China

"Truth in Testimony" Disclosure Form

In accordance with Rule XI, clause 2(g) of the Rules of the House of Representatives, witnesses are asked to disclose the following information. Please complete this form and attach it to your written testimony and it may be made publicly available in electronic format.

1. Date of Hearing:

2. Hearing Title:

3. Your Name:

4. Organization, organizations, or government entity you are representing:

5. Position title:

6. Are you an active registrant under the Foreign Agents Registration Act (FARA)?
   _____Yes _____No

False Statement Certification:

Knowingly providing material false information to this commission, or knowingly concealing material information from this commission, is a crime (18 U.S.C. 1001). This form may be made part of the hearing record.

_____

Witness Signature **Date**

Witness Biographies

Geoffrey Cain, foreign correspondent, author, technologist, and scholar of East and Central Asia

Geoffrey Cain has written for The Economist, the Wall Street Journal, Time, Foreign Policy, The New Republic and The Nation and is a contributing editor at The Mekong Review. He is a frequent guest on CNN, MSNBC, BBC, and Bloomberg. He is the author, most recently, of "The Perfect Police State: An Undercover Odyssey into China's Terrifying Surveillance Dystopia of the Future."

Samantha Hoffman, Senior Analyst at the Australian Strategic Policy Institute

Samantha Hoffman's work explores the domestic and global implications of the Chinese Communist Party's approach to state security. It offers new ways of thinking about understanding and responding to China's pursuit of artificial intelligence and big data-enabled capabilities to augment political and social control. Dr. Hoffman's analysis is widely sought after by governments across the world and media. She has publicly testified in the United States Congress, the House of Commons of the United Kingdom, and the European Parliament.

Yaqiu Wang, Senior Researcher on China at Human Rights Watch

Yaqiu Wang works on issues including internet censorship, freedom of expression, protection of civil society and human rights defenders, and women's rights. Her articles have appeared in Foreign Policy, The Atlantic, the Washington Post, and elsewhere. She has provided commentary to the BBC, CNN, the New York Times and others. Prior to joining Human Rights Watch, Wang worked for the Committee to Protect Journalists.

Jonathan Hillman, Senior Fellow with the Center for Strategic and International Studies

Jonathan Hillman is the director of the Reconnecting Asia Project, one of the most extensive open-source databases tracking China's Belt and Road Initiative (BRI). Prior to joining CSIS, Hillman served as a policy adviser at the Office of the U.S. Trade Representative, where he contributed to the 2015 U.S. National Security Strategy and the President's Trade Agenda and directed the research and writing process for essays, speeches, and other material explaining U.S. trade and investment policy. Hillman is the author, most recently, of "The Digital Silk Road: China's Quest to Wire the World and Win the Future" (HarperCollins, 2021).