STRATEGIC IMPORTANCE OF DIGITAL ECONOMIC ENGAGEMENT IN THE INDO-PACIFIC

HEARING

BEFORE THE

SUBCOMMITTEE ON ASIA, THE PACIFIC, CENTRAL ASIA, AND NONPROLIFERATION

OF THE

COMMITTEE ON FOREIGN AFFAIRS
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

JANUARY 19, 2022

Serial No. 117–98

Printed for the use of the Committee on Foreign Affairs

Available: http://www.foreignaffairs.house.gov/, http://docs.house.gov, or http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
46–522PDF WASHINGTON : 2022

COMMITTEE ON FOREIGN AFFAIRS

GREGORY W. MEEKS, New York, *Chairman*

BRAD SHERMAN, California
ALBIO SIRES, New Jersey
GERALD E. CONNOLLY, Virginia
THEODORE E. DEUTCH, Florida
KAREN BASS, California
WILLIAM KEATING, Massachusetts
DAVID CICILLINE, Rhode Island
AMI BERA, California
JOAQUIN CASTRO, Texas
DINA TITUS, Nevada
TED LIEU, California
SUSAN WILD, Pennsylvania
DEAN PHILLIPS, Minnesota
ILHAN OMAR, Minnesota
COLIN ALLRED, Texas
ANDY LEVIN, Michigan
ABIGAIL SPANBERGER, Virginia
CHRISSY HOULAHAN, Pennsylvania
TOM MALINOWSKI, New Jersey
ANDY KIM, New Jersey
SARA JACOBS, California
KATHY MANNING, North Carolina
JIM COSTA, California
JUAN VARGAS, California
VICENTE GONZALEZ, Texas
BRAD SCHNEIDER, Illinois

MICHAEL T. MCCAUL, Texas, *Ranking Member*
CHRISTOPHER H. SMITH, New Jersey
STEVE CHABOT, Ohio
SCOTT PERRY, Pennsylvania
DARRELL ISSA, California
ADAM KINZINGER, Illinois
LEE ZELDIN, New York
ANN WAGNER, Missouri
BRIAN MAST, Florida
BRIAN FITZPATRICK, Pennsylvania
KEN BUCK, Colorado
TIM BURCHETT, Tennessee
MARK GREEN, Tennessee
ANDY BARR, Kentucky
GREG STEUBE, Florida
DAN MEUSER, Pennsylvania
AUGUST PFLUGER, Texas
PETER MEIJER, Michigan
NICOLE MALLIOTAKIS, New York
RONNY JACKSON, Texas
YOUNG KIM, California
MARIA ELVIRA SALAZAR, Florida
JOE WILSON, South Carolina

SOPHIA LAFARGUE, *Staff Director*
BRENDAN SHIELDS, *Republican Staff Director*

SUBCOMMITTEE ON ASIA, THE PACIFIC, CENTRAL ASIA, AND NONPROLIFERATION

AMI BERA, California, *Chairman,*

BRAD SHERMAN, California
DINA TITUS, Nevada
ANDY LEVIN. Michigan
CHRISSY HOULAHAN, Pennsylvania
ANDY KIM, New Jersey
GERALD CONNOLLY, Virginia
TED LIEU, California
ABIGAIL SPANBERGER, Virginia
KATHY MANNING, North Carolina

STEVE CHABOT, Ohio, *Ranking Member*
SCOTT PERRY, Pennsylvania
ANN WAGNER, Missouri
KEN BUCK, Colorado
TIM BURCHETT, Tennessee
MARK GREEN, Tennessee
ANDY BARR, Kentucky
YOUNG KIM, California

JAMIE MORGAN, *Staff Director*

CONTENTS

STRATEGIC IMPORTANCE OF DIGITAL ECONOMIC ENGAGEMENT IN THE INDO-PACIFIC

Wednesday, January 19, 2022

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON ASIA, THE PACIFIC,
CENTRAL ASIA, AND NONPROLIFERATION
COMMITTEE ON FOREIGN AFFAIRS,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:08 a.m., via Webex, Hon. Ami Bera (chairman of the subcommittee) presiding.

Mr. BERA. Virtual gaveled in, and the Subcommittee on Asia, the Pacific, and Nonproliferation will come to order.

Without objection, the chair is authorized to declare a recess of the committee at any point. And all members will have 5 days to submit statements, extraneous materials, and questions for the record, subject to the length limitations in the rules. To insert something into the record, please have your staff email the previously mentioned address or contact full committee staff.

Please keep your video function on at all times, even when you are not recognized by the chair. Members are responsible for muting and unmuting themselves, and please remember to mute yourself after you finish speaking. Consistent with remote committee proceedings of H. Res. 8, staff will only mute members and witnesses as appropriate when they are not under recognition to eliminate background noise.

I see that we have a quorum and will now recognize myself for opening remarks.

First, I want to thank our witnesses and the members of the public for joining today's hearing on the importance of strengthening U.S. digital economic engagement with the Indo-Pacific region. The Indo-Pacific is home to many of our closest allies and significant trading partners, with more than 662 million people, and a combined of $3.2 trillion.

I have long supported deepening economic relations with our Indo-Pacific partners, and I believe we can do that in a way that protects and benefits American workers and strengthens the U.S. economy.

I also commend the Biden Administration for its continued prioritization of the region and its efforts toward developing an Indo-Pacific economic framework.

Today's hearing focuses on what I hope will be one important pillar in the broader economic framework: digital trading. The Indo-Pacific region contains the majority of the world's internet users and the fastest-growing internet market. The pandemic has only

further accelerated these trends. U.S. companies and platforms remain dominant in this expanding but increasingly competitive market, and further U.S. leadership is necessary to expand economic opportunities that improve the livelihoods of our workers and consumers in the United States and beyond.

As chair of the House Foreign Affairs Subcommittee on Asia and the Pacific, I do not intend for this hearing to examine what should be encompassed in a digital trade agreement, but, rather, I hope our witnesses will help talk about the geopolitical, economic, and strategic importance for the United States to engage our Indo-Pacific allies and partners on the development of standards for the digital economy and technology.

Countries in the region have long been negotiating and implementing digital trade policies to stimulate economic growth and improve the livelihoods of their citizens. Although these conversations occur thousands of miles away, they have significant implications for data protection and privacy, trade facilitation, and other issues that affect the American people and our economy.

But despite the wide-reaching impact of these agreements in today's interconnected economy, the United States is not at the table to ensure that the standards and norms being established align with our shared democratic principles. Our absence risks allowing countries that do not share our pro-worker, pro-consumer, pro small-business, and pro-environmental values to advance digital governance standards empathetical to democratic practices.

We need to engage our allies and partners to advance a prosperous Indo-Pacific region that supports a rules-based international trading system and high standards that prioritize openness and the free flow of data.

The United States has experienced negotiating digital trade chapters, which we did in the U.S.-Mexico-Canada agreement, and in the standalone U.S.-Japan digital trade agreement. These agreements provide for nondiscrimination, consumer protection and privacy and prohibit customs, duties, and technology transfer requirements among other obligations.

Working to lower barriers to digitally enable trade and establishing rules that allow for nondiscriminatory competition with Indo-Pacific countries will help U.S. companies compete more effectively.

I also want to be clear that this will need to be an inclusive process with the consultation of relevant stakeholders and groups. But the NAFTA renegotiation process demonstrated what is possible when all parties are at the table, and there is open dialog and compromises that ultimately strengthen the outcome that resulted in USMCA.

I have had the opportunity to hear from experts with differing opinions prior to today's hearing, and I look forward to continuing to work and have this conversation with labor and environmental groups to ensure that the U.S. digital economic engagement with the Indo-Pacific continues to be pro-worker, pro-environment, and pro-small business.

Our competitors are not waiting for us as they continue to shape the rules of the digital road in the Indo-Pacific. The United States has a unique window of opportunity to economically reengage the

region on this pivotal issue, and work with allies and partners to advance a free, open, and prosperous Indo-Pacific underpinned by our shared commitment to democratic norms and principles.

And I look forward to hearing from our witnesses today, as well as voices from other stakeholders and relevant industries, to ensure that we demonstrate sustained global leadership on these important issues.

Again, thank you to the witnesses and the members for participating today.

I will now yield 5 minutes to my good friend from Ohio, our ranking member, Representative Steve Chabot, for any opening comments he may have.

Mr. CHABOT. Thank you, Mr. Chairman. And I want to thank in advance the witnesses for sharing their insights with us here this morning.

It is hard to overestimate, as you have indicated, the strategic importance of the Indo-Pacific. The region accounts for about a third of global economic activity, has huge growth potential. With over half of the world's population and a youthful population at that, the region is poised to become an engine of global economic growth over the coming decades.

Moreover, the countries throughout the Indo-Pacific are hungry for trade, with the U.S., with each other, and with the rest of the world, and the world is hungry for trade with them. A free and open Indo-Pacific is critical to the U.S.'s economic future, as many of our largest trading partners are in the region, and there is enormous potential to grow those ties.

While the U.S. has strengthened our trade pacts with South Korea and Japan and developed bold standard rules on digital trade through the USMCA, we cannot rest on our laurels, but that is exactly what we are doing as Beijing continues to pressure Indo-Pacific countries to trade their sovereignty for the Chinese Communist Party's so-called common destiny, while we fail to provide a clear option for these countries to turn to.

Let me be blunt, Mr. Chairman, this Administration has no meaningful agenda for economic statecraft in Asia right now, and I say that with great remorse because we ought to be working together on this. And I know you and I are.

This brings me to the topic of today's hearing, the digital economy, which is comprised of the emerging tech, like AI, advanced semiconductors, and 5G. It is critical to superpower status in geopolitical competition. And this 21st century economic engine runs on data, a resource with infinite supply. Sustained and enhanced U.S. leadership in digital trade and innovation benefits not only our economy and work force, but our national security and economic well-being. That is why writing the rules around data and digital trade are so consequential. And, fortunately, we have templates in the U.S.-Japan trade agreement and in USMCA that would provide an ideal starting point for a high-quality deal.

That is why I was pleased to join you, Mr. Chairman, in leading a letter to USTR to ask that they move toward such a deal. From Zoom meetings to online shopping, to the increasing use of big data and AI in manufacturing sectors, the digital economy will only grow in importance to U.S. economic success.

All of these factors make the timing so appealing for a digital trade agreement in the Indo-Pacific. The consequences of inaction on digital trade with the region could be dire, as data and the digital economy are a matter of the utmost importance to Xi Jinping. The CCP, the Chinese Communist Party, grasps the value of data and is using it to coerce and control its trade partners. Over many years, the CCP has passed laws, regulations, and standards that give it control over the data of its companies and citizens, while at the same time, scouring the globe to funnel data back to China.

While we think a lot about ports and national resources, unfortunately, we have been too much asleep at the wheel as the world's most valuable resource, data, pours into the PRC every single day. That needs to change.

Mr. Chairman, it is time for us to get our heads in the game. And I agree with you that the best way to do this is to negotiate and conclude a digital trade agreement.

While I do have to admit that a digital sector agreement is a poor substitute for being part of the more comprehensive regional agreement, it is an excellent place to start building U.S. economic ties with our partners throughout the region.

Let me close with this: Across the Indo-Pacific, countries are hungry for more trade with the U.S., and we can achieve major foreign policy wins by meeting that demand. For example, Taiwan wants a trade deal so much that they finally allowed U.S. pork imports after years of delay. But whether it is digital trade or Taiwan, the Administration, unfortunately, has ignored the demand for real trade deals. Instead, they are poised to offer regional economic framework, which simply cannot meet the needs of the moment.

Let's hope the President decides to negotiate something more substantial, or I am afraid Americans will end up having to play by rules that were written in Beijing.

And I yield back.

Mr. BERA. Thank you, Ranking Member Chabot.

Let me now introduce our witnesses.

First we have Ms. Wendy Cutler, Vice President at the Asia Society Policy Institute. Ms. Cutler served for nearly three decades as a diplomat and negotiator in the Office of the U.S. Trade Representatives, where she also served as Acting Deputy U.S. Trade Representative.

Next, we have Ms. Christine Bliss, President of the Coalition of Services Industry. Prior to CSI, Ms. Bliss was Assistant U.S. Trade Representative for services, investment, telecommunications, and e-commerce.

Last but not least, is Mr. David Feith, adjunct senior fellow of the Indo-Pacific Security Program at the Center for a New American Security. He served as U.S. Deputy Assistant Secretary of State for East Asian and Pacific Affairs from 2020 to 2021.

I thank you all for participating in today's hearing.

I will now recognize each witness for 5 minutes. Without objection, your prepared written statements will be made part of the record. I will first invite Ms. Cutler for her testimony.

STATEMENT OF MS. WENDY S. CUTLER, VICE PRESIDENT, ASIA SOCIETY POLICY INSTITUTE

Ms. CUTLER. Well, thank you, Chairman Bera and Ranking Member Chabot, and distinguished members of the subcommittee. I am honored to have the opportunity to appear before you today, even if virtually.

As this subcommittee fully appreciates, the United States must strengthen its economic engagement in the Indo-Pacific. Given the trajectory of regional economic growth and innovation, U.S. prosperity is closely tied to the Indo-Pacific for the years to come. Without a robust regional economic agenda, the United States risks foregoing economic opportunities, and also becoming increasingly marginalized as the region forges a new future without us.

Furthermore, economic engagement will help strengthen U.S. credibility and influence in this pivotal region. Security partnerships alone will not achieve that. It is, therefore, encouraging that the Administration is now developing an Indo-Pacific Economic Framework.

Since the United States exited the TPP, our regional partners have not slowed down. In fact, the recent two regional comprehensive trade deals, CPTPP and RCEP, should serve as a wake-up call for Washington. And China's recent application to join the CPTPP is a potential game-changer and must be taken seriously. If the United States does not step up its economic game, CPTPP accession negotiations for China will become the most consequential negotiation in the region with the United States again sitting on the sidelines.

And our Indo-Pacific partners are also actively pursuing negotiations in the digital space. In addition to a series of bilateral trade agreements, Singapore, New Zealand, and Chile have concluded a partnership agreement which could become a platform for a broader regional deal, with Korea and China expressing interest in joining.

And now to turn to China, which is building a very different digital future. Indeed, Xi Jinping has described tech innovation as the main battleground of the global playing field. Just last week, China's State Council released an ambitious and detailed 5-year plan on digital aimed at bolstering the role of these technologies in its economy with goals related to broadband access, digital infrastructure, and emerging tech research. And, moreover, the plan lays out Beijing's international intentions, including partnering with ASEAN and the EU, as well as becoming more active on digital matters in international organizations.

China's goal is to leverage its gravitational pull of its economic heft to create a favorable international environment for its own digital vision, including policies related to cross border data flows, data privacy, and to the promotion of China-driven technical standards. And let's keep in mind that China's digital future includes worrying efforts to manage access to information, constrain dissent, and carry out monitoring and repression of certain populations.

The United States must work with like-minded countries to shape an affirmative alternative to the Chinese approach that advances democratic norms, including transparency, openness, interoperability, and fairness. And, in my view, there is no better way

to do this than by shaping a robust and forward-leaning digital pillar as the centerpiece of the Indo-Pacific economic framework.

Now, there are various approaches for doing this, but I believe the United States would be best served by proposing a new paradigm, and this would involve lifting the most meaningful, inclusive, and impactful elements from existing trade agreements, including the USMCA, while adding new features to promote digital inclusiveness, strengthen consumer confidence and trust, and protect personal information.

The goal should be to ensure that the outcomes serve the interests of our workers, consumers, and businesses of all sizes, particularly SMEs. And, moreover, a digital economy pillar should be sufficiently flexible to take on the challenges presented by new trends and technologies, including AI and worker force skill development.

In pursuing such an approach, extensive consultations with Congress and all stakeholders are critical in order to get this right. And to be impactful as possible, an agreement should include flexibilities to cast a wide net for potential membership, particularly in Southeast Asia where tech is booming and Chinese tech companies have been aggressively expanding their presence in recent years.

In conclusion, Mr. Chairman, a bold, meaningful, and impactful, and inclusive Indo-Pacific economic framework with a strong digital pillar could go a long way in reasserting U.S. leadership and influence in the region; but time is of the essence. We need to move now to help shape the economic future of the region, or risk becoming observers as others do.

Thank you.

[The prepared statement of Ms. Cutler follows:]

Testimony before the

House Foreign Affairs Committee

Subcommittee on Asia, the Pacific, Central Asia, and Nonproliferation

Hearing on

"Strategic Importance of Digital Economic Engagement in the Indo-Pacific"

Testimony by Wendy Cutler

Former Acting Deputy U.S. Trade Representative

January 19, 2022

Chairman Bera, Ranking Member Chabot, distinguished members of the Subcommittee, thank you for the opportunity to appear before you today to share my thoughts on the importance of a bold and impactful U.S. economic agenda for the Indo-Pacific region, with a digital economy component as its centerpiece.

No one understands better than this Subcommittee the geopolitical and economic significance of the Indo-Pacific region. As Secretary Blinken recently remarked, "The Indo-Pacific will, more than any other region, shape the trajectory of the world in the 21st century."

The Indo-Pacific is home to some of the largest, most dynamic and fastest-growing economies in the world. The region accounts for over 60 percent of global GDP and over one-third of global goods trade, up from 25 percent a decade ago. For the United States this means two-way trade with the region of over $1.75 trillion, making it the destination for nearly one-third of U.S. exports and supporting over 3 million American jobs. As we look ahead, the Indo-Pacific is poised to be the powerhouse of economic growth and innovation for years to come. Between 2019 and 2050, over half of global growth is expected to come from this region. Moreover, the region is projected to account for the majority of the global middle class by mid-century, making it a significant driver of future demand for goods and services.

The United States must strengthen its economic engagement in the Indo-Pacific. Given the trajectory of regional economic growth and innovation, U.S. economic prosperity will be closely tied to the region for the years to come. Without a robust regional economic agenda, the United States risks foregoing economic opportunities and becoming increasingly marginalized as the region forges a new future without us. As the global economy's center of gravity shifts towards the Indo-Pacific, the rules of regional economic engagement will help shape global rules and norms, whether or not we help to craft them.

Furthermore, robust economic engagement is also essential to restore U.S. credibility and influence in the Indo-Pacific. Security partnerships alone will not achieve that. Our regional partners are looking to the United States to offer a constructive and credible economic vision. It is therefore encouraging that the Administration is now developing a new Indo-Pacific Economic Framework (IPEF) to be launched early this year.

THE CHANGING INDO-PACIFIC TRADE LANDSCAPE

Since the United States exited the TPP, our regional partners have not slowed down in their quest for open markets and new economic opportunities. They view trade expansion as an essential path to promote economic growth, create jobs, and improve livelihoods for their citizens. The fact that two mega-regional trade deals have now entered into force over the past three years without the United States is stunning in light of where these countries were only a decade ago. It should serve as a wake-up call for the United States. No longer are our partners waiting for us to lead the charge. With a new-found confidence, they are working among themselves, including with China, to strengthen trade, investment and supply chain ties.

Just three weeks ago, the Regional Comprehensive Economic Partnership, or RCEP, entered into force for the ten Asian members who have ratified the agreement. The remaining five signatories are in different stages of their domestic ratification procedures but are expected to join soon. With this agreement in force, China is now part of the world's largest trading bloc covering a market of 2.2 billion people and roughly 30 percent of today's global GDP. The CPTPP recently marked its third anniversary, with eight of its eleven members having brought this high-standard agreement into force. The year ahead will be critical in determining the future shape and direction of CPTPP as members consider four pending accession applications from the United Kingdom, China, Taiwan, and Ecuador. Several other countries, including South Korea, may join the queue for membership soon.

China's CPTPP application is a potential game changer and must be taken seriously. There is no doubt that given its current trade and investment regime China would have major difficulties in adhering to many existing CPTPP rules. However, that is not a reason to dismiss the prospect of accession by the world's second largest economy. China is the number one trading partner for most countries in the region, with trade and investment flows growing steadily, and supply chains strengthening in many sectors. While some CPTPP members will try to strictly hold China to the same terms and the same high standards as any other member, others are already signaling more flexibility, believing that this would be a promising opportunity for further market-opening and reform by Beijing, while increasing their access to the large and growing Chinese market. If the United States does not step up its economic game, CPTPP accession negotiations for China could eclipse all other regional initiatives and become the most important trade negotiation in the region, with the United States sitting on the sidelines.

In addition to comprehensive trade deals like RCEP and CPTPP, our Indo-Pacific partners are also aggressively pursuing sectoral agreements, with negotiations in the digital space accelerating at an unprecedented pace. In 2020, Singapore signed its first digital agreement with Australia and in just the past six weeks, has concluded similar agreements with the United Kingdom and Korea. It is also embarking on a new digital partnership with the European Union. Singapore, New Zealand and Chile have also partnered to conclude the Digital Economy Partnership Agreement (DEPA) which is envisioned as a platform for a broader regional deal. DEPA has been gaining momentum, attracting interest from Canada and formal applications to join from South Korea and most recently China. Asian countries are also active in shaping multilateral digital rules, with Australia, Japan, and Singapore leading the ongoing plutilateral e-commerce negotiations at the WTO involving more than eighty WTO members.

ADVANCING THE INDO-PACIFIC ECONOMIC FRAMEWORK

There is no question that given the choice, most, if not all of our regional partners would prefer that the United States return to the CPTPP. However, they are coming to terms with the reality that this is unlikely to happen anytime soon, if ever. While the Biden Administration is not interested in pursuing a traditional market-opening trade agreement, it recognizes the urgency of strengthening its economic engagement in this vital region and is now developing a plan for engagement -- the Indo-Pacific Economic Framework (IPEF). So far, this initiative has been discussed in generalities, touching upon a range of topics, including the digital economy and technology, resilient supply chains, decarbonization, infrastructure, and worker standards. Agencies are now busy fleshing out the details and looking to advance the initiative in the region over the course of this year.

In my conversations with counterparts in the region, I sense a degree of skepticism that the Framework will be sufficiently substantive and receive the sustained attention by senior Administration officials to make it as impactful as a trade agreement. Moreover, I have picked up in my discussions a genuine concern that whatever specific initiatives Washington proposes under the IPEF, they will pale in comparison to China's move to join the CPTPP. At the same time, given that they want the U.S. back in the region with a substantive economic agenda, our partners are trying to keep an open mind.

The onus is now on Washington to develop a credible alternative that will simultaneously serve U.S. economic interests and attract partners with tangible benefits for shared prosperity, innovation, and inclusive growth. In my view, there is no better way to achieve these objectives than by proposing a robust and forward-leaning digital pillar as the centerpiece of the Framework.

IMPORTANCE OF A DIGITAL AGENDA

Why is digital so critical? The benefits of digitization are by no means limited to the services sector or to the big data companies. In fact, digital technologies touch all sectors of our economy impacting workers, small businesses, farmers, and consumers. For example, manufacturing relies on big data analytics, additive manufacturing, and supply chain management to modernize traditional processes and increase productivity. Likewise, farmers are utilizing digital technologies, such as artificial intelligence and the Internet of Things (IoT) to more efficiently and sustainably manage agricultural resources

Moreover, the COVID-19 pandemic has accelerated a shift to reliance on digital technologies in all aspects of our daily life, from healthcare delivery to remote work and learning. Furthermore, digital technologies have served as a lifeline for small and medium-sized enterprises (SMEs), allowing many to continue to serve their customers both domestically and internationally. There is no turning back from this tide. The International Data Corporation forecasts that 65% of global GDP will be digitized by the end of this year. To some extent, almost every industry can be considered a digital industry today.

There is nowhere in the world where the digital economy is more important than in the Indo-Pacific. Asia already accounts for half of the world's internet users and digitization of their societies is rapidly growing. The Asian Development Bank forecasts that Asia will account for 40 percent of the increase in global GDP due to digitization between 2021 and 2025. These digital trends are creating opportunities for businesses of all sizes and will shape the future economic parameters of the Indo-Pacific.

TIME IS OF THE ESSENCE

Amidst this explosion of the use and application of digital technologies, the region is not waiting for the United States to join in crafting the new rules of the road for the digital age. They are being hammered out as we speak, both bilaterally and in groupings of countries. Absent U.S. participation, these rules may work against our interests. Indeed, we are already seeing this – a case in point being the broad exception provided in the RCEP E-Commerce chapter where data obligations can essentially be ignored if a party decides for itself to do so under the guise of a self-judging public policy exception. To prevent such provisions and exceptions from becoming the regional norm and spreading to other agreements, U.S. leadership is critical.

Another crucial factor is China, which is building a very different digital future. Just last week China's State Council released an ambitious five-year plan for the digital economy, aimed at bolstering the role of digital in the Chinese economy overall, with goals related to emerging tech research, digital infrastructure, broadband access and more. China's approach to digital is marked by laws and regulations requiring data localization, restrictions on cross-border data flows, and policies that favor and promote domestic digital champions. But the digital economy is not bound by geographic borders, so no matter how domestic the focus, China's efforts are inherently international in their implications.

Indeed, the State Council's plan is explicitly framed as "a key force in reorganizing global resources, reshaping the global economic structure, and altering the global competitive landscape." It lays out Beijing's intentions to pursue digital economy partnerships with ASEAN and the EU, as well as to become more active on digital matters in international organizations, including the WTO. China's goal is to create a favorable international environment for its own priorities related to cross-border data flow restrictions, data privacy, market access and more. And China's vision for the use of digital technologies includes worrying efforts to manage access to information, constrain dissent, and carry out monitoring and repression of certain populations. The United States must work with like-minded partners to provide an affirmative alternative to this approach that advances democratic norms and values, such as transparency openness, and fairness.

At the same time, protectionist digital measures have been the rise. USTR's 2021 National Trade Estimate (NTE) report highlights a range of recent policy and regulatory actions undertaken by Asian countries, including data localization requirements, discriminatory practices affecting trade in digital products, and restrictions on the provision of digital services. Experience has shown that it is always harder to reverse course once policies become enshrined in domestic legal and regulatory frameworks. We have the opportunity now to help write the rules to discipline such measures, which ultimately hurt our businesses and workers.

DEVELOPING AN INDO-PACIFIC DIGITAL ECONOMY AGREEMENT

There are a number of options on how best to pursue a regional digital economy strategy. For example, the United States could seek membership in the DEPA or alternatively could ask partners to sign on to the U.S.-Japan Digital Agreement. However, I believe that the United States would be best served by shaping a new paradigm by lifting the most meaningful, inclusive, and forward-looking elements from existing agreements, while adding new features to better ensure that the outcomes benefit all of our citizens, and don't accrue disproportionately to large companies. In developing such an approach, extensive consultations with Congress and stakeholders, including labor, consumer groups, and NGOs,

are critical. But in pursuing these conversations, it's important to be mindful of which suggestions might be more appropriately addressed by the implementation of domestic measures rather than in an international pact.

In my view, there are five core areas for a proposed digital economy agreement:

First, the *values and principles* underlying the overall agreement should be included up-front. The October 2021 G-7 Digital Trade Principles provide some useful and relevant ideas, including the importance of an open, free and secure internet; the need for digital markets to be competitive, transparent, fair and accessible; the view of digital trade as a tool to support jobs, raise living standards and respond to needs for workers, innovators, and consumers; and a rejection of digital protectionism.

Second, certain provisions of *existing digital trade agreements* should be featured. In this regard, the CPTPP, U.S.-Japan Digital Trade Agreement, and the digital chapter of the USMCA can serve as important models. Among the provisions to be included would be free flow of data across borders; prohibition on localization requirements for computing facilities; and a ban on requirements to turn over one's source code, algorithms, or related IPR. These provisions would promote innovation and economic growth while ensuring that U.S. products and services, which are among the most competitive in the world, are treated fairly in foreign markets.

Third, new or expanded provisions should be added to *address concerns of workers and consumers*, including those that promote digital inclusiveness; strengthen consumer confidence and trust; and protect personal information. In addition, a venue for discussing the development of needed workforce skills for the digital world, a challenge facing all economies, would be beneficial.

Fourth, such an agreement should focus on *promoting those digital tools that enhance the ability of SMEs to market, sell, and receive payments for their products and services*. It should include provisions to facilitate trade by enabling paperless trading, e-invoicing and e-bills of lading.

Fifth, a digital economy pact should be designed to *take on challenges presented by new trends and technologies*. Given the dynamic nature of this sector, an agreement cannot be static if it is to remain relevant. This can start with "soft" provisions featuring exchanges on such trends, including the emergence and application of artificial intelligence.

POTENTIAL PARTNERS FOR A DIGITAL ECONOMY AGREEMENT

Finally, to be impactful, an agreement should cast a wide net for potential membership while still seeking to keep standards high. While it may be tempting to move forward with only those countries that already share our values and interests in the digital space, this is not the optimal approach. Instead, Washington should try to be as inclusive as possible as it contends with competing views for the digital future so that our vision is well-positioned to prevail.

In particular, the U.S. should make special efforts to encourage ASEAN member countries to get on board. With a large and youthful population, Southeast Asia is projected to grow over 5.5% annually to become the fourth largest economy in the world by the end of this decade. ASEAN's digital economy is a key driver of this rapid growth with over 400 million internet users and an internet economy that is projected to reach $1 trillion by 2030. ASEAN also hosts a vibrant ecosystem of digital companies with

many opportunities for U.S. businesses. Governments in ASEAN are prioritizing digital development as well, with an ASEAN E-Commerce Agreement entering into force at the end of last year.

A more inclusive digital agreement may require offering some flexibilities to attract members. DEPA can serve as a possible model. It features a "modular" structure with countries having the option of joining the agreement in its entirety or just signing up for certain parts as a first step. Adopting some version of this approach is worth considering.

CONCLUSION

The time is now for the United States to demonstrate its interest and resolve in pursuing strong and enduring economic engagement in the Indo-Pacific region. Reasserting U.S. economic leadership won't be easy given the recent dramatic changes in the regional economic landscape. Our partners have developed the confidence to move forward without us and are busily working among themselves to set regional rules, norms and standards, irrespective of our participation. That said, a bold, meaningful and inclusive economic framework with a strong digital component could a go a long way in getting us back to the regional rule-making arena.

As was so well stated in a recent letter by the Chairman and Ranking Member and signed by a number of members of this Subcommittee, "a digital trade agreement with like-minded countries in the Indo-Pacific region presents a unique opportunity to expand American economic leadership in the region and improve lives" but "this window of opportunity will not remain open indefinitely." I could not agree more. We need to move now to position the United States as a regional leader on these matters.

Thank you.

Mr. BERA. Thank you, Ms. Cutler.

I will now recognize Ms. Bliss for her testimony.

I do not know if your camera is on, Ms. Bliss. There it is. Great.

STATEMENT OF CHRISTINE BLISS, PRESIDENT, COALITION OF SERVICES INDUSTRY

Ms. BLISS. Chairman Bera, Chairman Meeks and Ranking Member McCaul, as well as subcommittee Ranking Member Chabot, and distinguished members of the subcommittee, I appreciate the opportunity to participate in today's hearing to discuss the strategic importance of digital economic engagement in the Indo-Pacific.

My name is Christine Bliss. I am president of the Coalition of Services Industry, and we represent services and digital firms on services and digital trade issues. Our members include firms that provide information technology services, financial services, logistics, media and entertainment, distribution, and professional services.

I want to note at the outset that CSI supports the Biden Administration intention to develop an Indo-Pacific framework to renew U.S. leadership in the world's fastest growing region, as you noted, Mr. Chairman, in your opening remarks. We believe that all potential aspects of the IPEF, including digital trade, sustainability, supply chain, resilience, and labor are all important. However, in line with the topic of today's hearing, my testimony focuses on the significance of the digital economic engagement pillar.

An Indo-Pacific trade agreement has received bipartisan congressional support, thanks to the leadership of this committee and you, Mr. Chairman, and other Members of Congress that recognize the strategic imperative of taking swift action to reassert U.S. leadership in the region.

I would also note, as you did, Mr. Chairman, in your opening remarks, that I believe that USMCA provides a positive process and precedent for the IPEF in light of its broad, bipartisan support, and robust stakeholder engagement, including with the labor community and others.

As Ms. Cutler noted in her testimony, and you did in your opening remarks and Ranking Member Chabot's opening remarks, digital engagement in the Indo-Pacific region is an urgent exercise.

First, expansion of services in digital trade with the region is critical to supporting existing and future jobs and services in digital sectors in the United States, as well as in supporting manufacturing and other key sectors of the U.S. economy.

And this is not just about moving the interests of large U.S. services and digital firms and professional workers. It is also about creating new opportunities for the 52 million U.S. workers in services occupations earning middle class wages, which can benefit from the creation of new jobs in digital and digitally enabled services, and to their participation in supply chains.

It is also vitally important to micro-, small and medium-sized businesses which increasingly depend on access to broadband, internet platforms, and the latest digital applications in the cloud to expand their domestic and international reach.

Second, digital engagement in the region is essential to combat rising protectionism, even among our closest allies in the region.

Data localization and data residency requirements are proliferating, and they do not only pose major trade barriers, but they also enable increased authoritarian influence, censorship, and surveillance, and leave networks vulnerable to cybersecurity risks.

U.S. engagement in the region's digital economy is also important to counteracting China's protectionist and authoritarian whole-of-government approach to shaping the rules of the road on digital trade.

Ms. Cutler alluded to the recently announced 5-year plan by China to even tighten its grips on data sovereignty and to expand its reach on digital policies internationally.

China also recently concluded the RCEP and had a great influence on the standards on digital trade in that regard, which were incredibly weak. And this is important because RCEP is the world's largest trading block, accounting for 30 percent of global GDP.

China's application to accede to regional agreements like CPTPP and the digital economy partnership are also of great concern.

Additionally, as has been noted, U.S. allies, like Japan, the U.K., Australia, Singapore, New Zealand, Korea, and other nations are expanding their digital networks while the U.S. is not, and is at serious risk of being left behind. In the words of Singapore's Deputy Prime Minister, Heng See Keat, the U.S. cannot afford to be absent from the regions involving the economic architecture, if not through CPTPP, then it must have an equally substantial alternative.

Finally, the digital aspects of IPEF and any associated digital agreement should include world class digital provisions applying to all services sectors. It should promote worker skill training, particularly for women, small businesses, and historically marginalized communities. The IPEF should be accompanied by a regional digital agreement with like-minded allies, including Japan, Singapore, Australia, New Zealand, and Korea and should be binding and enforceable.

My written testimony also includes an annex recommending specific provisions to be included in such an agreement.

In conclusion, Mr. Chairman, I thank you for the opportunity to testify today and appreciate the subcommittee's attention to these critical issues.

[The prepared statement of Ms. Bliss follows:]

Hearing before the United States House of Representatives Committee on Foreign Affairs, Asia, the Pacific, Central Asia, and Nonproliferation Subcommittee

"Strategic Importance of Digital Economic Engagement in the Indo-Pacific"

Christine Bliss

President

Coalition of Services Industries

January 19, 2022

Chairman Meeks and Ranking Member McCaul, subcommittee Chairman Bera and Ranking Member Chabot, thank you for the opportunity to appear before you today to discuss the strategic importance of digital economic engagement in the Indo-Pacific.

My name is Christine Bliss, and I am the President of the Coalition of Services Industries, a non-profit trade association that represents the international objectives of the U.S. services sectors. Our members include companies that provide services both domestically and internationally, including information and communication technology services, financial services, express delivery and logistics, media and entertainment, distribution, and professional services. CSI members operate in all 50 states and over 100 countries.

Allow me to frame my comments by first stating support for the Biden administration's intention to develop an Indo-Pacific Economic Framework (IPEF) to demonstrate renewed U.S. leadership in the world's fastest growing region, which accounts for 60 percent of global GDP, and is home to longstanding U.S. economic partners and the world's three fastest growing emerging economies.

While we believe that all potential aspects of the IPEF, including digital trade, sustainability, supply chain resilience and labor are all important, my testimony focuses on the importance of the digital trade component of the IPEF in line with the topic of today's hearing. Indeed, it is my belief that high-standard digital trade commitments with economic partners that share our values can make a significant contribution to the Biden Administration's Build Back Better World agenda by supporting economic growth that is inclusive, fair, and sustainable, while promoting core democratic values, raising living standards, and creating new economic opportunities for people domestically and globally.
Strong digital trade principles and binding disciplines in the IPEF and an associated digital agreement are critical not only to services and digital firms, both large and small, but also to reinforcing supply chain resilience, solutions to address climate change, and the promotion of worker rights. Trade in digital goods and services are very interdependent; promoting one also reinforces and promotes the other.

Importantly, an Indo-Pacific digital trade agreement has received bipartisan Congressional support thanks to the leadership of this Committee and other members of Congress in both chambers that recognize the strategic imperative of taking swift action to reassert U.S. leadership in the Indo-Pacific region. I also note that USMCA provides a strong model for inclusive and robust stakeholder engagement, a process which undoubtedly contributed to its passage with unprecedented bipartisanship and the endorsement from the labor community.

This is an urgent exercise for multiple reasons. Digital and services trade barriers are on the rise: U.S. companies are increasingly at a disadvantage because of digital protectionist policies and unfair support from non-market economies. This will come as no surprise to Members of this Committee. But particularly concerning is that we are seeing a proliferation of blatantly discriminatory policies from some of our closest allies. Companies in China are making strategic investments in digital infrastructure across the globe, supported by massive subsidies and low interest loans that skew the market and disadvantage American offerings. Increased Chinese investment in e-commerce and other digital goods and services in the region pose serious risk to U.S. security interests. Data localization and data residency requirements are also proliferating, placing U.S. companies, workers, and innovators at an

even greater disadvantage. These policies also create opportunities for increased authoritarian influence and censorship, while leaving networks vulnerable to cybersecurity risks and interference.

All the while, China has launched a whole of government effort to export its economic model and shape the rules of the road for digital trade. In fact, just last week, the Chinese government released a 5-year digital economy plan, which aims to make China less reliant on foreign partners while its partners' resilience on China increases. China has also ramped up its activities in multilateral institutions like the WTO and the International Telecommunications Union (ITU), as well as bilaterally and regionally, recently concluding the Regional Comprehensive Economic Partnership (RCEP) which represents 30% of global GDP and entered into force on January 1st. And of course, China recently submitted its application to accede to the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and to join the Digital Economy Partnership Agreement (DEPA). It is vitally important that RCEP's digital disciplines—which are weak, self-judging and replete with exceptions—do not become the rules of the road on digital trade in the Asia Pacific. In particular, RCEP's provisions regarding data localization, restrictions on cross-border data flows, and policies that champion domestic industry are highly concerning and will not provide an effective means to rein in China's discriminatory, authoritarian approach to digital regulation. U.S. allies like Japan, the UK, Australia, Singapore, New Zealand and nations other than the United States are expanding their networks of digital trade disciplines and innovative new approaches. The U.S. is at serious risk of being left behind.

American trade and economic leadership in the region is sorely needed. A U.S.-led high-standard digital trade agreement in the Indo-Pacific region will advance Biden Administration foreign policy goals to promote the interests of micro-, small and medium-sized enterprises (MSMEs), middle class workers and also facilitate greater economic inclusion in the U.S. and Asia Pacific region. MSMEs increasingly depend on access to broadband, internet platforms, and the latest digital applications in the cloud to expand their domestic and international markets. U.S. workers, particularly middle-class workers, also benefit from the creation of new jobs in digital and digitally enabled services and through their participation in supply chains. To have a meaningful impact in promoting the current benefits and future growth of digital flows in the region, the Administration's Indo-Pacific Economic Framework must include strong digital principles and binding disciplines, as well as market access commitments. In the words of Singapore's Deputy Prime Minister Heng See Keat, "the U.S. cannot afford to be absent from the region's evolving economic architecture" – "if not through the CPTPP, then it must have an equally substantial alternative." With that in mind, we offer the following recommendations on the scope and shape of the IPEF itself and any subsidiary digital trade agreement along with specific provisions we believe should be both reflected in overall principles and commitments in the IPEF and any subsidiary digital trade agreement.

Scope

Digitally related aspects of the IPEF and any associated digital agreement should include world class provisions applying to all sectors, including services and financial services sectors, with no exclusion of audiovisual services or digital content. It should cover all aspects of digital trade flows and digitally

enabled services and technologies—including protection of cross-border data flows; prohibitions on data localization and mandatory transfer of source code and algorithms; measures to expand government access to open government data; commitments to use international standards, coverage of paperless trade and measures to facilitate interoperability in areas such as digital identity, electronic authentication, and electronic signatures; and to promote cybersecurity and interoperable approaches to personal data protection as well as coverage of newer areas such as principles regarding ethical use of AI And measures to promote data innovation such as regulatory sandboxes. It should also include investments in digital skill training to ensure that workers have the necessary skills to succeed in the digital economy while advancing the promotion of digital trade opportunities for women and small businesses.

Architecture

Indo-Pacific Framework

We understand that the IPEF is likely to consist of two parts: a broad political level framework with a large group of Indo-Pacific countries and associated bilateral or regional agreements. With regard to the broad IPEF framework, longstanding trade principles of non-discrimination, transparency, openness and interoperability should take center place. Such a framework should also include a consultation mechanism and other means to raise member concerns and to hold members accountable. On digital trade, we believe it should include a political commitment to a standstill and rollback with regard to digital trade barriers.

Economic Agreements

The cornerstone of the IPEF should be a regional digital agreement with like-minded countries that will establish high standard digital disciplines. All Indo-Pacific nations that are willing to agree to high-standard principles and binding commitments should be included, and we believe that the Biden Administration should prioritize including Japan, Australia, Singapore, New Zealand, and Korea in this group. We are skeptical about India's willingness to meet such high standards.

We believe it is important to avoid a patchwork of non-binding bilateral TIFAs, which might have differing provisions and would overall have less force in combatting the rise of digital protectionism in the region. Therefore, we believe that any digital agreement under the IPEF should be binding and enforceable, and include coverage of all sectors.

Substantive Provisions: Digital Principles and Disciplines for Promoting Inclusiveness and Growth

A digital trade agreement under the IPEF should cover core elements of the USMCA digital trade and financial services chapters, the U.S.-Japan Digital Trade Agreement, the Singapore-Australia Digital Economy Agreement, as well as disciplines and principles included in updated digital chapters in Australian FTAs, recently concluded UK FTAs with Singapore and Australia, and the Digital Economy

Partnership Agreement. These contain innovative new provisions for easing trade barriers for SMEs and services, and the creation of a regulatory sandbox for work on emerging technologies and digitally enabled services. It should also align with and enhance efforts to realize Data Free Flows with Trust (DFFT) and expand the APEC Cross-Border Privacy Framework system. We also recommend a political level standstill and rollback commitment with *respect to data localization and other protectionist digital measures*. These principles and disciplines will generate benefits for workers and SMEs and facilitate greater economic growth in the U.S. and Indo-Pacific regions. We have enclosed an Annex with a comprehensive list of suggested principles and disciplines for a digital trade agreement as part of the IPEF. Below we highlight key elements.

Principles

A. Liberalization of digital trade

The benefits of liberalized digital trade for both SMEs and U.S. workers have been well-documented.[1] Due to enhanced productivity and lower trade costs, digitally intensive industries have led to increased U.S. GDP, job creation and increased real wages. As detailed by the ITC, "[h]igher demand for workers in the digitally intensive industries drives up wages in the labor market, draws workers from other sectors of the economy, and can also increase aggregate employment as more workers are brought into the labor force."[2] Access to online marketplaces and online stores enables companies of all sizes to export. Cloud services democratize access to technology, enabling minority- and women-owned small businesses and startups to scale their businesses faster and more seamlessly. Liberalized (digital) trade has been demonstrated to provide SMEs with access to diversified markets and new consumers, and to increase sales.[3] Digital trade agreements also promote investment in the U.S. economy by innovative companies that understand the tremendous potential of such agreements to grow their global customer base.

Digital and services firms are a core element of domestic and international supply chains. As noted in a 2019 McKinsey Report on the role of services in supply chains, supply chains are becoming increasingly digitized and data driven. In addition, services and digital technologies are critically important to

---

[1] *See, e.g.*, U.S. International Trade Commission, *Digital Trade in the U.S. and Global Economies, Part 2*, August 2014, available here, p. 17; Congressional Research Service, *Digital Trade and U.S. Trade Policy*, May 2019, available here, pp. 7-8 (and the studies cited therein).
[2] US International Trade Commission, *Digital Trade in the U.S. and Global Economies, Part 2*, available here, p. 16.
[3] *See, e.g., What Do CPTPP Member Country Businesses Think about the CPTPP?*, Kati Suominen, Centre for Strategic and International Studies, August 2021, available here, pp. 2-5 (finding that the surveyed SME online sellers in the CPTPP region report an increased ability to diversify into new markets, with 51% of micro (1-10 employees) online exporters and 36% of small (11-50 employees) online exporters reporting increased sales).

manufacturing in terms of both the manufacturing process itself in terms of robotics, data analytics and use of smart technologies and supporting manufacturing exports and competitiveness.

B. Trade facilitation through digital trade agreements

Recently negotiated digital trade agreements include trade facilitation obligations that benefit U.S. companies, including SMEs, by lowering export costs and red tape at the border through digital tools. U.S. companies, including SMEs that export, are more productive, more competitive and pay higher wages.[4] Increased access to inputs and technology from foreign markets also allows U.S. SMEs to increase productivity, and manufacture and export more sophisticated high-value products.

C. Trust in the digital economy

Along with its tremendous benefits and efficiencies, digital trade creates certain risks for the consumers and SMEs that rely on it.[5] Through digital trade agreements, countries can reduce such risks and inject trust into the digital economy by recognizing the importance of consumer protection in digital trade, developing principles and standards that can promote trust in emerging technologies and use consistent with democratic norms, and otherwise limiting the dangers that can potentially arise from online transactions.

D. Promoting Inclusion in the digital economy

The newest generation of trade agreements has begun to include provisions that promote inclusiveness of the digital economy. Through these provisions, parties emphasize that the benefits from digital trade should be equitably shared throughout the population of each of the parties, regardless of race, gender, or socioeconomic status. U.S. digital trade agreements should aim to ensure that no U.S. worker or consumer is left behind as technology advances and digital trade increases.

E. Sustainability

An Indo-Pacific digital agreement could advance the Biden Administration's sustainability objectives. Provisions could establish commitments for parties to provide open access to energy markets for renewable electricity suppliers, consumers, and corporate buyers and link those markets across borders; increase consumer options for sourcing renewable energy beyond the existing grid mix; and promote common accounting tools to track renewable energy such as renewable energy certificates (REC) or other similar instruments. Such provisions could enable U.S. investors and local companies alike to reach renewable energy goals across the region.

Conclusion

The suggested elements to be included in an IPEF and a regional digital Asia Pacific agreement are intended to encourage further discussion and development of a robust digital agenda for the region. The principles could be used in whole or in part on a binding or hybrid binding and non-binding approach.

I thank you for the opportunity to testify today and the committee's attention to these critical issues.

ANNEX: Digital Principles and Disciplines for Promoting Inclusiveness and Growth

Liberalization of digital trade

1. PROHIBITING DIGITAL CUSTOMS DUTIES
2. SECURING BASIC NON-DISCRIMINATION PRINCIPLES particularly with respect to digital products, content and services.
3. SECURING ROBUST MARKET ACCESS COMMITMENTS ON INVESTMENT & CROSS-BORDER SERVICES, INCLUDING THOSE DELIVERED DIGITALLY
4. ENABLING CROSS-BORDER DATA FLOWS consistent with regulations based on legitimate public policy objectives.
5. PREVENTING LOCALIZATION BARRIERS
6. BANNING FORCED TECH TRANSFERS & PROTECTING CRITICAL SOURCE CODE AND ALGORITHMS
7. FOSTERING INNOVATIVE ENCRYPTION PRODUCTS
8. ENSURING TECHNOLOGY CHOICE
9. PROMOTING A FREE & OPEN INTERNET
10. SUPPORTING DATA INNOVATION
11. ADVANCING STRONG & BALANCED PROTECTION OF IP RIGHTS
12. PROMOTING TRANSPARENCY & STAKEHOLDER PARTICIPATION IN THE DEVELOPMENT OF REGULATIONS & STANDARDS.
13. PROMOTING SUPPLY CHAIN RESILIENCY

Trade facilitation through digital trade agreements

14. ENCOURAGE EXPORTS OF GOODS SOLD ONLINE WITH HIGHER TAX-FREE & TARIFF-FREE THRESHOLDS
15. ADVANCING INNOVATIVE AUTHENTICATION METHODS
16. ENABLE PAPERLESS TRADE
17. REQUIRING CROSS-BORDER INTEROPERABILITY OF E-INVOICING SYSTEMS
18. ENHANCING SECURE & INTEROPERABLE E-PAYMENT SYSTEMS
19. FOSTERING DIGITAL TRADE THROUGH INTERNATIONAL STANDARDS

Trust in the digital economy

20. ENSURE ENFORCEABLE CONSUMER PROTECTION
21. ENSURE ADEQUATE PROTECTION OF PERSONAL DATA
22. PROMOTE COOPERATION ON CYBERSECURITY
23. CREATE A SAFE ONLINE ENVIRONMENT
24. DEVELOPING ETHICAL & GOVERNANCE FRAMEWORKS FOR THE USE OF AI TECHNOLOGIES

Inclusiveness of the digital economy

25. WORK TO INCREASE TRADE & INVESTMENT OPPORTUNITIES FOR SMES, AND CREATE NEW JOBS FOR WORKERS
26. ENSURING LABOR RIGHTS ARE A KEY CONDITION FOR LIBERALIZATION OF TRADE (INCLUDING DIGITAL TRADE)
27. RECOGNIZE DIGITAL INCLUSION AS A DRIVER OF ECONOMIC & SOCIAL DEVELOPMENT:
28. MUTUAL RECOGNITION OF DIGITAL IDENTITIES
29. PROMOTING EQUALITY OF OPPORTUNITY IN DIGITAL ECONOMY
30. INCREASING ACCESS TO RETRAINING & DIGITAL SKILLS
31. COOPERATION ON DIGITAL CAPACITY BUILDING

Mr. BERA. Thank you, Ms. Bliss.

I now invite Mr. Feith for his testimony.

STATEMENT OF DAVID FEITH, ADJUNCT SENIOR FELLOW, INDO-PACIFIC SECURITY PROGRAM, CENTER FOR A NEW AMERICAN SECURITY

Mr. FEITH. Thanks very much, Chairman Bera, Ranking Member Chabot, and all the distinguished subcommittee members. I appreciate very much the opportunity to speak with you about digital trade with the Indo-Pacific, and, more broadly, the strategic importance of data rules.

I wish to stress three main points today:

First, a U.S. digital trade agreement in the Indo-Pacific would indeed serve American interests economically and strategically.

Second, such an agreement is, by no means, all that is needed. Our country should improve our overall approach to digital trade, starting by curbing the massive and currently unregulated frozen sensitive data from the United States to China.

Third, U.S. diplomacy should seek to cooperate with allies on both of these tracks, to expand digital trade among friends and to limit it with China.

The case for expanding U.S. digital trade in the Indo-Pacific is strong, as we have heard, because digital trade is important, and the Indo-Pacific is important. There are various ways that we can craft better digital trade rules in the Indo-Pacific and, as we have discussed, the general contours of a desirable deal are visible from previous U.S. agreements. Parties would agree not to impose tariffs on each other's digital content; parties would agree not to force technology transfers as a condition of market access; parties would agree in general to open cross border data flows, meaning they would limit data localization. The more that our Indo-Pacific allies partners honor rules like these, the better for regional economic development and for U.S. interests.

There are notable risks in our current approach, however. It is not nearly enough to expand digital trade with our partners. We also need to limit our digital trade with China. Our most urgent digital trade challenge, in fact, may not be in the Indo-Pacific, but at home. It is how to begin placing overdue national security controls on data flows to and from China.

China's approach to digital trade has long been far more strategic, mercantilist, and nonreciprocal than U.S. policy has recognized. The Chinese Communist Party has developed comprehensive strategy to control, accumulate, and exploit data, data such as personal health records, personal genetic sequences, and personal online browsing habits; data such as corporate trade secrets, corporate supply chain records, and corporate financial accounts; data such as the photos, voice recordings, and mapping imagery pulsed through phones, drones, and smart cars all throughout the world.

Beijing recognizes that the competition for global influence in the 21st century will require protecting and harnessing this data to achieve commercial, technological, military, and intelligence advantages. And that is what it is doing.

As we have heard, Beijing has built a latticework of laws and regulations to make the Chinese Communist Party effectively the

world's most powerful data broker. This has a huge impact on foreign firms operating in China. Not only must their Chinese data stay in China and be accessible by the Chinese State, but Beijing now demands control over whether they can send it to their own headquarters, or to a corporate lab in, say, California, or to a foreign government that has made a lawful, regulatory, or law enforcement request.

Beijing's approach is nakedly nonreciprocal. It relies on access to data from foreign countries while denying foreigners access to data from China. In China, Beijing controls the data of foreign companies. Outside of China, Chinese companies operate comfortably, creating and accessing valuable new data sets prime for easy transfer back to China in all manner of data-intensive fields, biotech, pharma, medical devices, drones, autonomous cars and trucks, social media, digital payments, e-commerce, and more. These data flows to China contain massive quantities of American information.

All of this is the stuff of digital trade, yet there are effectively no rules governing any of it. In this environment for upwards of a generation, Beijing has been coldly effective in designing a strategy of global data mercantilism: data hoarding for me, data relinquishing for thee.

The Biden Administration has spoken about the importance of data in our competition with China, but no visible strategy has yet emerged. The U.S. Government traditionally has no mechanism for limiting cross-border data flows, even on national security grounds.

When an American teenager wants to download a Chinese social media app onto her phone, or a U.S. university wants to exchange biotech research with a Chinese university, or U.S. State Government wants to use Chinese drones for power grid surveillance, the U.S. Government has no way to regulate this activity to protect American important interests.

Washington is beginning to address this gap only recently due to creation, at least on paper, of the new ICTS regulatory regime for reviewing cross-border data flows. But the ICTS process has not yet been put to use. Apart from ICTS, the Congress could, of course, consider legislative approaches, and various bills have been proposed to limit the ability of Chinese social media apps to operate and collect data in the U.S., but without success.

Another idea is to create a new export control regime that would restrict bulk personal data from going to foreign adversaries, but that, too, has not garnered much apparent support.

I will close by noting quickly how, as we struggle to develop new standards for our own digital trade with China, it will be difficult to harmonize our approach with partners overseas. But overcoming this challenge is essential if we are to create a favorable global digital order.

We have discussed China's interest in joining the CPTPP. China wants to do so chiefly to influence its currently high standards and to protect, thereby, China's more mercantilist and authoritarian interests. CPTPP members have a veto over this and should use it.

Important as it is, however, to keep Beijing from entering CPTPP against the rules will hardly be sufficient for shaping the future of trade in Asia. As we have said, fashioning a high standard Indo-Pacific digital trade agreement would be a good step, and so would

begin to impose reasonable national security restrictions on U.S.-China data flows.

The concept that combines these two elements, digital trade expansion with friends and digital trade limitation with rivals, is what former Japanese Prime Minister Shinzo Abe called Data Free Flow with Trust. We should maximize data trade with those we can trust, and limit data trade with those we cannot. This will not be easy, given China's size, strength, and deep integration into our digital economy and that of our allies, but it is necessary.

Our responsibility now, now that we recognize increasingly that data is a strategic resource, is to design a global digital trade order that reflects democratic values and not Beijing's.

Thank you very much, Mr. Chairman.

[The prepared statement of Mr. Feith follows:]

David Feith
Adjunct Senior Fellow, Center for a New American Security
Former Deputy Assistant Secretary of State for East Asian and Pacific Affairs

Testimony before the U.S. House Foreign Affairs Committee
Subcommittee on Asia, the Pacific, Central Asia, and Nonproliferation
"The Strategic Importance of a U.S. Digital Trade Agreement in the Indo-Pacific"

January 19, 2022

Chairman Bera, Ranking Member Chabot, and the other distinguished Subcommittee Members: I appreciate this opportunity to speak with you about digital trade with the Indo-Pacific and, more broadly, the strategic importance of data rules. Thank you for your invitation.

It is a rare pleasure nowadays to deal with an issue on which there is strong bipartisan common ground. Many Democrats and Republicans in the House and Senate, including from this Subcommittee, have together urged the Biden Administration to pursue new arrangements for expanding digital trade with America's partners in the Indo-Pacific.

I wish to stress three main points today:

> First, a U.S. digital-trade agreement in the Indo-Pacific would indeed serve American interests economically and strategically.
>
> Second, such an agreement is by no means all that is needed. Our country should improve its overall approach to digital trade – starting by curbing the massive and now unregulated flows of sensitive data from the United States to China.
>
> Third, U.S. diplomacy should seek to cooperate with allies on both of these tracks – to expand digital trade among friends, and to limit it with China.

The Importance of Indo-Pacific Digital-Trade Expansion

The case for expanding U.S. digital trade in the Indo-Pacific is strong because digital trade is important, and the Indo-Pacific is important. The digital economy accounts for some 10% of U.S. GDP; digital trade contributes more to U.S. GDP than financial or merchandise flows; and digital trade is growing faster than traditional trade in goods and services.[1] The Indo-Pacific, meanwhile, is the world's most economically and strategically important region. The United States has vital interests there, and strong allies and partners with whom we share the strategic imperative of preventing China from achieving regional hegemony.

[1] https://sgp.fas.org/crs/misc/R44565.pdf

Increasing economic engagement with Indo-Pacific partners is a key U.S. objective. Digital trade is a ripe and valuable area to prioritize in this regard. Expanding digital-trade flows, and improving digital-trade rules, would be good for the U.S. economy, good for answering the region's strong demand for greater U.S. economic engagement, and good for long-term U.S. strategy.

As we will surely discuss, there are various ways we could craft better digital-trade rules in the Indo-Pacific. We could build on existing arrangements, such as the 2019 U.S.-Japan Digital Trade Agreement, the digital-trade chapter of the U.S.-Mexico-Canada Agreement (USMCA), and/or the U.S.-Australia free trade agreement of 2005. We could also seek to join the evolving Digital Economic Partnership Agreement (DEPA) involving Singapore, New Zealand and Chile, and/or the Singapore-Australia digital trade agreement of 2020.

The general contours of a desirable deal are visible from previous U.S. agreements. Parties would agree not to impose tariffs on each other's digital content. They would agree not to force technology transfer as a condition of market access (meaning companies would not be required to reveal source code or encryption keys just to participate in digital trade). Parties would agree, in general, to open cross-border data flows (meaning they would limit "data localization" rules requiring that data be stored locally and barred from transfer overseas). And parties could harmonize policies on such matters as labor rights, digital inclusion, and digital-market facilitation for small and medium-sized businesses.

The more that our Indo-Pacific allies and partners honor these rules, the better for regional economic development and for U.S. interests. That's why there is strong bipartisanship in Congress on these issues, and on urging the Administration to prioritize digital trade and data governance in its Indo-Pacific Economic Framework.

The Limits of Indo-Pacific Digital-Trade Expansion

There are notable risks in our current approach, however. To set new global rules for the data age, and to compete with China, it is not nearly enough to expand digital trade with our partners. We also need to limit our digital trade with China. The trade with China gives rise to grave threats to our security and hampers our ability to forge appropriate global rules.

Our most urgent digital-trade challenge may not be in the Indo-Pacific but at home. It is how to begin placing overdue national-security controls on data flows to and from China. Without this, the benefits of improving digital-trade rules with our friends in the region could be far outweighed by the costs of our failure to get our U.S.-China data-trade house in order. Indeed, unless we set better, clearer "rules of the road" at home, our ability to shape such rules abroad will be severely limited.

A necessary first step is understanding China's approach to digital trade, which has long been far more strategic, mercantilist, and non-reciprocal than U.S. policy has recognized. This U.S. blind spot is increasingly damaging.

For nearly a decade, Chinese leader Xi Jinping has spoken of data as the oil of the 21st century—the indispensable input that will fuel economic strength and national power. In 2013, he told his state-run Chinese Academy of Sciences:

> *The vast ocean of data, just like oil resources during industrialization, contains immense productive power and opportunities. Whoever controls big data technologies will control the resources for development and have the upper hand.*

The analogy between data and oil later became something of a cliché in certain circles. But U.S. policy never adjusted to recognize its logic. China's did.

The Chinese Communist Party developed a comprehensive strategy to control, accumulate, and exploit data. Data such as personal health records, personal genetic sequences, and personal online browsing habits. Data such as corporate trade secrets, corporate supply chain records, and corporate financial accounts. Data such as the photos, voice recordings, and mapping imagery pulsing through phones, drones, and smart cars all around the world.

Beijing recognizes that the competition for global influence in the 21st century will require protecting and harnessing this data to achieve commercial, technological, military and intelligence advantages. And that's what it is doing.

Beijing has built a latticework of laws and regulations to make the Chinese Communist Party the world's most powerful data broker. A set of laws implemented in 2017 asserted the Party's unchecked power to gain access to private data on Chinese networks, whether in China or associated with Chinese firms such as Huawei overseas. Last year, Beijing enacted a new set of laws that go even further, by demanding not just access to private data but effective control over it.

This has a huge impact on foreign firms operating in China. Not only must their Chinese data stay in China and be accessible by the Chinese state, but Beijing now demands control over whether they can send it to their own headquarters; or to a corporate lab in, say, California; or to a foreign government that has made a lawful regulatory or law-enforcement request. Beijing's new laws may make it criminal to comply with foreign sanctions against China that involve data – like shutting off banking or cloud services to a Chinese entity linked to human rights atrocities. In these cases, foreign firms can comply with U.S. law, or they can comply with Chinese law, but not both.

The impact of these laws is clear. Tesla, Apple and others have opted to build dedicated Chinese data centers – sometimes in partnership with Chinese state entities, lest they lose access to the large Chinese consumer market and valuable manufacturing supply chain.

Beijing's bullying data rules inside China complement its longstanding efforts to buy, steal, and otherwise acquire data from foreign sources outside of China. Beijing hacks foreign corporate

databases. It runs "talent recruitment" programs at foreign universities and firms. It buys foreign companies. And it funds its own data-driven companies to conduct research, forge partnerships, win customers, and vacuum up data in open foreign markets like Silicon Valley, Boston, and Austin.

Beijing's approach is nakedly non-reciprocal. It relies on access to data from foreign countries while denying foreigners access to data from China. In China, Beijing controls the data of foreign companies. Outside of China, Chinese companies operate comfortably, creating and accessing valuable new data sets primed for easy transfer back to China in all manner of data-intensive fields – biotech, pharmaceuticals, medical devices, drones, autonomous cars and trucks, social media, digital payments, e-commerce, and more. These data flows to China contain massive quantities of information about American citizens, American companies, American government, and American critical infrastructure.

All this is the stuff of digital trade, yet there are effectively no rules governing any of it. There is nothing effective under the World Trade Organization or any U.S.-China bilateral trade accord, and not under U.S. domestic law either, where we have no comprehensive federal approach to data governance. Because of the nature of the internet – namely, that it was able to expand globally in a permissive environment, without any of the state controls inherent with traditional goods transported by truck or ship – digital trade (including U.S.-China digital trade) has remained fundamentally unregulated.

In this environment, for upwards of a generation, Beijing has been coldly effective in designing a strategy of global data mercantilism: data hoarding for me, data relinquishing for thee. If the United States and our allies don't organize an effective response, Beijing will succeed in commanding the heights of future global power. Any new digital-trade arrangements we make with our Indo-Pacific friends would still operate in the shadow of a global digital-trade order that is fundamentally lawless and fatally exploitable by Beijing.

The Domestic Regulatory Imperative

The Biden Administration has spoken about the importance of data in our competition with China. "Our strategic competitors see big data as a strategic asset, and we have to see it the same way," said National Security Adviser Jake Sullivan last summer. But no visible strategy has yet emerged.

The U.S. government has traditionally had no mechanism for limiting cross-border data flows, even on national-security grounds. Traditional national-security restrictions on commerce are designed to address other issues, and they have historically been narrowly scoped, consistent with important American traditions of limited government. The Committee on Foreign Investment in the United States (CFIUS) screens inbound investment. Export controls restrict outbound flows of U.S. goods and technology. Procurement restrictions limit what federal government departments and agencies can buy.

But vast areas of economic life are untouched by those tools – including the cross-border exchange of data by private companies, individuals, academic institutions, and state and local governments. When a U.S. medical-device company wants to buy Chinese hardware and software for its U.S. operations, or an American teenager wants to download a Chinese social-media app onto her phone, or a U.S. university wants to exchange biotech research with a Chinese university, or a U.S. state government wants to use Chinese drones for power-grid surveillance, the U.S. government has no way now to regulate this activity to protect important American interests.

Washington has begun to address this gap only recently, through the creation – at least on paper – of a new regulatory regime for reviewing cross-border data flows. Known as "ICTS" (for Information and Communications Technology and Services), this regime was established in the waning days of the Trump administration and maintained by the Biden administration through a June 2021 executive order on "Protecting Americans' Sensitive Data From Foreign Adversaries." Under the ICTS process, an interagency panel, led by the Commerce Secretary, has broad discretion to investigate, modify, block, or unwind data-related commercial transactions believed to present "undue or unacceptable risks" to U.S. national security.

This ICTS panel has authority across six sweeping sectors: critical infrastructure; network infrastructure, including satellites, wireless networks, and cable access points; data hosting, including services with the personal information of more than one million Americans; surveillance and monitoring technology, including drones; communications software, including mobile and gaming apps; and emerging technologies, including artificial intelligence and autonomous systems. These sectors touch nearly the entire modern economy.

But the ICTS process has not yet been put to use – not against Chinese access to U.S. data centers or biotech labs, not against Chinese drones with eyes on U.S. critical infrastructure, and not against other channels through which large volumes of sensitive U.S. data can flow to China. (A press report this week that the Administration is scrutinizing Chinese e-commerce giant Alibaba's cloud business on data-security grounds point to what ICTS enforcement might look like, but so far the report is unconfirmed.)

Apart from ICTS, the Congress could of course consider legislative approaches. Various bills have been proposed limiting the ability of Chinese social-media apps to operate and collect data in the United States, but without success. Another idea is to create a new export-control regime that would restrict bulk personal data from going to adversary countries. So far, however, such measures have not garnered much support. The issue of Beijing's data mercantilism appears absent from the China-focused U.S. Innovation and Competition Act (USICA) that passed the Senate last June, is pending before the House, and focuses on other matters such as boosting U.S. domestic semiconductor manufacturing.

Elsewhere on Congress's agenda, there is the risk that efforts intended to rein in domestic Big Tech platforms could end up imposing stricter standards on American firms than on Chinese

ones, which would be perverse from the perspective of both commercial competition and U.S. national security.

The International Path to 'Data Free Flow with Trust'

As we struggle to develop new standards for our own digital trade with China, it will be difficult to harmonize our approach with partners overseas. Overcoming the challenge, however, is essential, if we are to create a favorable global digital order.

Consider Europe. Across effectively the entire era of digital trade, we have been at cross-purposes with our European allies over data-privacy rules, while far greater data-related harms from Beijing have mounted. In Europe and beyond, Chinese companies processing European data are theoretically subject to localization and privacy-protection requirements under the European Union's General Data Protection Regulation (GDPR). But the EU has to date shown no great concern with mass data collection and exploitation by Chinese companies functioning as extensions of the Chinese state.

In the Indo-Pacific, the dynamic is more fluid, which is part of the reason why we could benefit from entering the fray. The 11-nation Comprehensive and Progressive Trans-Pacific Partnership (CPTPP) includes high digital standards consistent with those of the U.S.-Japan Digital Trade Agreement and USMCA. Were we to secure an Indo-Pacific digital deal along these lines, we may be able to cement these high standards, at least among like-minded countries.

Beijing wants to block that outcome. It prefers lower digital-trade standards, like those in the Regional Comprehensive Economic Partnership (RCEP) agreement, to protect its mercantilist and authoritarian interests. That is why it is now pushing formally to join both the high-standard CPTPP and the non-binding but potentially high-standard DEPA – to try to shape (that is, restrain) their standards from the inside. Beijing realizes that digital-trade flows are still overwhelmingly unregulated, and it wants to influence whatever might emerge to fill this international regulatory gap.

Beijing's CPTPP bid is not just cynical but subversive. In just about every category that should matter, Beijing doesn't meet the agreement's standards. Certainly not in digital trade. But also not in labor rights, environmental protection, state-owned enterprises, or basic respect for trade rules in the first place (like those of the WTO, or of Beijing's free trade deal with Australia, which it violates daily with its lawless embargo on Australian goods). But Beijing is powerful, so it demands that CPTPP members let it in anyway.

Some in Washington believe that CPTPP countries cannot be expected to hold the line and exclude Beijing for too long. But why concede that point? If rules-based trade means anything, it means not letting Beijing corrupt yet another institution such as CPTPP. A critical mass of CPTPP members – Japan, Australia, Canada, others – ought to be able to uphold its principles. Failing to do so could be a decisive blow to hopes for securing proper trade standards rather than rules made by and for China.

Important as it is, however, keeping Beijing from entering CPTPP against the rules will hardly be sufficient for shaping the future of trade in Asia. Fashioning a high-standard Indo-Pacific digital-trade agreement would be a good step. So would visibly beginning to impose reasonable national-security restrictions on U.S.-China data flows, followed by consultations to encourage partners to do the same.

The concept that combines these two elements – digital-trade expansion with friends, digital-trade limitation with rivals – is what former Japanese Prime Minister Shinzo Abe called "Data Free Flow with Trust" (DFFT). We should maximize data trade with those we can trust and limit data trade with those we cannot. In other words, more data flow among democratic allies and other like-minded countries, and less data flow with China.

DFFT is a simple notion that will be hard to implement given China's size, strength, and deep integration into our digital economy and that of our allies. It is necessary, however. We are overdue in recognizing data as a strategic resource. Our responsibility now is to design a global digital-trade order that reflects democratic values and not Beijing's.

*Note: Some of the language above is adapted from an op-ed co-authored by David Feith (with Matt Pottinger), "China Is Winning the Big Data War," New York Times, November 30, 2021.

Mr. BERA. Great. Thank you.

I will now recognize members for 5 minutes each. And pursuant to House rules, all time yielded is for the purposes of questioning our witnesses.

Because of the virtual format of this hearing, I will recognize members by committee seniority, alternating between Democrats and Republicans. If you miss your turn, please let our staff know, and we will circle back to you. If you seek recognition, you must unmute your microphone and address the chair verbally.

With that, I will start by recognizing myself.

Again, I appreciate the work that the ranking member, Mr. Chabot, and I have been doing on this, as well as the other subcommittee members.

And, Ms. Cutler, your opening testimony—I know both of us worked together during the Obama Administration to get TPA passed and TPP. And, you know, it was a somewhat contentious deal and, ultimately, we did not get it across the finished line.

That said, in the last Administration, you know, there was a lot of work on the renegotiation of NAFTA. All parties were brought to the table. I have had conversation with some of the labor negotiators and others, and everybody did not get what they wanted, but it did demonstrate a process and, ultimately, led to a strong bipartisan vote where I think in the House, there were more House Democrats that actually voted for that bill than House Republicans.

So it does show an open process with all stakeholders at the table, labor, environmental groups, you know, the business community, and others, that we can actually get a trade deal across the finish line. So it is, again, something that we are very supportive of the Biden Administration pursuing.

Maybe the first question would go to Ms. Cutler. You outlined a few of the existing policies. There is a digital trade capture in the USMCA. There is the bilateral that we have between the United States and Japan. You also touched on the Singapore, New Zealand, Chile deal, which, you know, seems to be a more modular deal. If you can expand on these different, you know, options and potentially where a good starting point would be?

Ms. CUTLER. Yes. So as you mentioned, there is so much digital activity going on in the region. Singapore has really been instrumental in seeking bilateral agreements with other countries, and they recently concluded a deal with Korea. At the same time, Singapore is part of this regional effort with Chile and New Zealand with this so-called Digital Economy Partnership Agreement.

And I think all of—these agreements in the region without us, as well as drawing from the USMCA and U.S.-Japan Bilateral Digital Agreement, really provides a great starting point for the United States. I do not think we should dock on to any of the agreements in the region, because I think they all need to be updated and improved and reflect more effectively labor and consumer concerns that we are hearing in the United States.

But my sense is that our regional partners and allies are very excited about working with us in this area. They are not waiting for us, but they are welcoming.

Mr. BERA. Great. Thank you for that.

I have to, you know, second that. I cannot have a conversation with Australians or our friends in New Zealand or Singapore or Indonesia without this topic coming up, and there really is a strong desire in the region for the United States to engage and help come up with a high-standard agreement that really does set the rules of the road.

Mr. Feith, you talked a little bit about some of the risks, you know, what China is doing in terms of data privacy and the like. Can you outline, you know, or maybe expand on the risks that we face if we do not actually set a high standard, you know, trade deal?

Mr. FEITH. Certainly. The risks if we fail to set standards in the region include that China's model, which it inherently uses to exert influence over not just foreign companies, but foreign countries, the approach of foreign countries to not just matters of economics and trade, but also, you know, matters of political and foreign policy decisionmaking, Beijing will have a freer hand to dictate terms. They can do that either by getting inside these institutions, as we have discussed. If these institutions, like CPTPP, do not hold by their own standards, if they were, over the years, to be pressured by Beijing to make the decision that, even though it would, frankly, make nonsense of the rules and standards that CPTPP is supposed to stand for, to bring in China when China's data regime is what it is, when China's labor regime is what it is, when its approach to State-owned enterprises is what it is. But, obviously, these forces are subject to politics. And Beijing will indeed be pressing to work its way in both inside these institutions, or from the outside, if the institutions are not sufficiently strong, Beijing will be able to exert itself on other countries and will not have the collective market and, sort of, policy power of these countries working together in these trade blocks exerting influence on Beijing, which over time we would prefer.

Mr. BERA. I have noticed my time has expired, so thank you for that.

Let me go ahead and recognize the ranking member, Mr. Chabot, for 5 minutes.

Mr. CHABOT. Thank you, Mr. Chairman.

Mr. Feith, I will begin with you.

Neither this Administration, nor the previous one, showed particular interest in new trade deals in the Indo-Pacific. That has essentially left the State Department to champion economic engagement, which it has been attempting to do, but without the heft of the USTR.

What opportunities are we missing in the region with the White House holding USTR on such a tight leash?

Mr. FEITH. Well, thanks for that, Congressman Chabot.

The experience that I had in Singapore reflected very much what you said, and I will say, to the extent that we are speaking broadly about economic engagement with the Indo-Pacific, it is worth noting that, you know, in addition to the tools that we have, formal trade negotiation tools that obviously are led by USTR, in addition to some of the general economic and diplomacy tools that are wielded by the State Department, there are additional very important tools, including some that have been sharpened and strengthened

by this committee over the years, to include the International Development Finance Corporation, and the Eximbank. These are both also important for making sure that American trade investment in this vital region are as substantial as possible and, therefore, American influence is, too.

But I think, as your question suggests, there is still a power in broad trade deals properly negotiated that can be, you know, among the strongest tools that we have. And it is interesting the ways that in different Administrations and sometimes with continuity across Administrations, the dynamics between the White House, USTR, and State function.

One thing we observed in the last Administration with some interest was questions about whether the bandwidth constraints of USTR, in terms of personnel and the number of hours in the day, could be mitigated through personnel transfers where, you know, larger parts of the government, like the State Department or others, could lend personnel to build out trade missions, the ability to visit more countries and have more negotiations.

Those were, I think, interesting issues which merit additional consideration if I could suggest that.

Mr. CHABOT. Thank you.

Let me ask you this: What consequences do we face if we fail to compete with China in the trade arena, relative to our economy, to strategic competition more generally? I will just leave it there.

Mr. FEITH. Well, you know, China under Xi Jinping has a fundamentally different view of the future of the world than we do, and that our allies and partners all around the world do. They have a, frankly, intensely adversarial and hostile view toward our interests and our values.

So to the extent that we accede competitive ground to them, to the extent that we let them continue to advance in their economic and technology goals without competing properly, without making power cells more resilient against their subversion, without making our allies and partners stronger and more resilient in that fashion, the consequences could be absolutely severe for control in generally in Asia, and globally.

Mr. CHABOT. Thank you.

Ms. Bliss, let me try and get a question, one more in here. History shows, I believe, that the wealthiest countries tend to be those that have been successful in the trade arena.

Could you discuss some of the economic benefits of the U.S. if we could negotiate a digital trade deal with countries in the Indo-Pacific?

Ms. BLISS. Absolutely. Thank you, Congressman Chabot.

So it is critically important for services and digital trade and the firm—services and digital firms that I represent, and, more broadly, in the economy, but also because those firms also support other economic sectors, like agriculture, like manufacturing.

And as I think you noted in your opening remarks, there is tremendous growth potential in the Asia Pacific, particularly in countries like Malaysia and Vietnam, Indonesia. And so, the digital aspect of that is very, very important to creating and supporting U.S. jobs in digital and digitally enabled services-related areas.

Just to give you an example, U.S. services digital exports are $500 billion. Out of that, just in the Asia Pacific, $180 billion in services exports, $124 billion of that total are digital. And that is just the beginning. We believe there is tremendous growth potential there in that regard.

So the benefits of tapping into the region with strong digital rules are tremendously important and, as I noted, not just to the large firms and services in digital trade, but also, to the smaller firms, in particular, that rely on digital tools to expand their reach to domestic and to global markets and, particularly, women and minorities. 90 percent of minority businesses are small businesses. And so the benefits, I think, are quite large.

If I can add a couple of things to, I think, a question that you asked and also that the chairman asked, in terms of the consequences of not having a strong Indo-Pacific strategy in counteracting China, also include the fact of China's widening influence in multilateral institutions, whether it is the WTO, APEC, or the ITU and in standard settings bodies in particular.

So, an Indo-Pacific digital agreement, MOU, whatever form it would take, should include addressing standards for digitally enabled services, because that is another area where we really face a huge challenge from China.

And then, finally, I also wanted to emphasize, with respect to China, that China heavily influenced the outcome in the RCEP negotiations. And as a result, the digital disciplines are, unfortunately, full of exemptions, and they are quite weak, particularly in areas such as data localization, restrictions on cross-border data flows, and provisions that champion domestic industries.

So we do not want that to become the model throughout the Asia Pacific region. So I know I went beyond the specific outlines of your question, but I just wanted to add a couple of points to the question that you and the chairman raised.

Mr. CHABOT. Thank you.

Mr. BERA. The gentleman's time has expired.

Let me go ahead and recognize the gentleman from California, Mr. Sherman, for 5 minutes of questioning.

Mr. SHERMAN. I would ask that you go to the next Democrat and have me be the Democrat after that.

You are muted, Mr. Bera.

Mr. BERA. Let me recognize the gentleman from Michigan, Mr. Levin, for 5 minutes of questioning.

Mr. LEVIN. Thanks so much, Mr. Chairman. This is a really important hearing.

I want to focus on some of the privacy concerns associated with the digital trade components of the agreements we have been discussing here today.

Today's tech giants have a nearly unfettered ability to collect, store, transfer, and use personal data from their customers around the world for their own profit. The U.S. has thus far failed effectively to regulate the tech sector here at home to ensure that consumer privacy rights are protected, particularly compared to European data regulations.

Ms. Bliss, in your testimony, you express support for a, quote, "U.S. led high standard digital trade agreement in the Indo-Pacific region," end quote.

Could you expand on what those high standards would look like in practice, particularly when it comes to privacy rights, please?

Ms. BLISS. Well, thank you, Congressman.

I think that you are absolutely right that privacy protection is extremely important, and I will say that I think action on Federal privacy legislation is very important as part of that and as a foundation to address the patchwork of State-level privacy laws that exist now.

So just foundationally, I think that is an important point.

I think that there are important privacy-related provisions that have been included in the USMCA and other agreements——

Mr. BERA. Ms. Bliss, if you could turn your camera on.

Ms. BLISS. Sorry about that.

I do think there are important provisions that have been included in previous digital provisions, agreements such as USMCA, the U.S.-Japan agreement, for example, ensuring that parties have an adequate privacy framework domestically. I think——

Mr. LEVIN. Could I just ask you, Ms. Bliss, does your organization represent the big tech companies, the tech giants of the United States? Are they part of your organization?

Ms. BLISS. There are—I do have a number of tech companies that are members. They are not the majority of my membership by any means; but, yes, they are included.

Mr. LEVIN. Some of, like, Alphabet and whatever Facebook calls itself now, or Apple, or, you know, Amazon, any of those?

Ms. BLISS. Not Apple, but yes, I do have.

Mr. LEVIN. Does your coalition support European privacy protections?

Ms. BLISS. No, we have not taken a position on that.

Mr. LEVIN. I see.

Ms. BLISS. However, we have been of the view that it is possible to ensure privacy protection in a way that recognizes the European right to enforce the GDPR, in terms of working out trade rules, digital trade rules with respect to cross-border data transfer.

Mr. LEVIN. OK. Let me try to get in one more question. That is helpful. Thank you.

So U.S. competition with China obviously looms large in this discussion, particularly in terms of setting standards, the rules of the road for future digital trade norms and practices. And, obviously, China's own initiatives in its participation in multilateral agreements are already shaping the digital trade sphere as some of you have said.

Let me ask, Ms. Cutler, how can we ensure that U.S. engagement in digital trade and future agreements does not perpetuate a race to the bottom in terms of competitive business standards? And what policies or norms would you suggest that we champion in digital trade agreements that would allow us to compete effectively with China but still protect consumer rights, the privacy rights I was talking about before?

Ms. CUTLER. Well, thank you, Congressman Levin.

That is a good question, and I emphasize in my testimony that I really think we need an affirmative agenda here. This is not about—we should not just focus on countering China, but let's set the stage for what is important to us. And protection of data is important. Cross-border data flows is also important. Digital inclusiveness is important. The norms of nondiscrimination and fairness is important.

So, in my view, that is kind of the approach we should take. Of course, in the back of our minds is China, but that cannot be the driver. We should, again, assert an affirmative positive agenda, and I think that will gain a lot more traction in the Indo-Pacific region with our allies and partners and, frankly, other countries that are kind of sitting on the fence.

Mr. LEVIN. All right.

Thanks, Mr. Chairman. Looks like my time has expired. I yield back.

Mr. BERA. Thank you.

Let me now recognize the gentleman from Pennsylvania, Mr. Perry, for 5 minutes of questioning.

Mr. PERRY. Thank you, Chairman Bera.

For any of our panelists who might want to answer, I would like to glean a little more information as to the expectations for a bilateral trade agreement with Taiwan. I mean, given the fact that Taiwan has repeatedly demonstrated its good faith interest in negotiating with the United States, what do you think is the appetite within the Biden Administration for a free trade agreement with Taiwan? And do you think we can expect anything like that within the next few years? Any panelist that wishes to answer that.

Ms. CUTLER. Perhaps I will take a shot at it, and I cannot speak for the Biden Administration, and I do not know exactly where they are in these discussions. But what I have gleaned from my conversations with Administration officials is that there is a real commitment to strengthen, expand, and deepen our economic relations with Taiwan. And just in the past year we have seen, for example, USTR reinvigorate the TIFA, the Trade Investment Framework Agreement, set up working groups. We have seen the State Department and Commerce also set up bilateral channels dealing with supply chains, technologies, green technologies, et cetera.

So I think there is robust and unprecedented economic engagement with Taiwan. And, again, I cannot speak, you know, is that sufficient or is the Administration envisioning, you know, that at some point maybe, when they are ready to do free trade treatments, that they would look to Taiwan to conclude such an agreement.

Mr. PERRY. Okay. Thank you.

Anybody else wish to weigh in?

Ms. BLISS. I would just—Congressman, I would just say I would agree with Wendy's assessment that I think that given the current Administration's reluctance to at least at this point proceed with trade agreements, probably that may not be realistic in the near term to expect. However, as Wendy pointed out, there has been a much higher level and interest in engagement in various ways with Taiwan, which I think is encouraging.

So that seems to be the likeliest outcome, at least in the near term.

Mr. PERRY. All right. I mean, I appreciate the sentiment. I just—I feel like we are tiptoeing—and, look, you are just here to help inform us, but we are tiptoeing around the circumstance with Taiwan and China trying to not offend China; at the same time, China has no problem offending us or the rest of the world, and we have got a great trading partner right next door that has been honest and true with us all along, and I just—personally, I do not—I think we ought to be more robust and forceful in that.

But given maybe what I would the consider the Administration's dithering establishing trade policies in the Indo-Pacific, and to me, that maybe indicates a lack of consensus among U.S. officials, but do you guys think that individual trade agreements, digital trade agreements with some of the friendly partner nations is a plausible way to go as opposed to something far more reaching?

You know, do you think that that is—do you think that the individual trade agreements is what we really have to hope for with some of these more allied countries to us?

Ms. BLISS. Congressman, I would just respond by saying that it appears that the Administration is pursuing bilaterally with some key allies in the region, whether it be Singapore or others, that be making a visit to Indonesia and have been in Indonesia, and will be going to ASEAN.

So that seems to be the approach, bilateral approach. However, I think from our perspective, we would hope, at least with respect to digital trade, that there would be the prospect for a regional digital agreement to avoid a patchwork of agreements that could have differing standards.

I think there are obviously negative commercial implications of that of having differing standards, but there is also, I think, the China angle too, which is, I think, a regional digital agreement would have stronger force and the ability to counteract some of the negative policies that we have been talking about with respect to China.

So, again, I think it is a preference rather than a reflection of where the Administration is. But I think, from our perspective, we would hope that there is the possibility of doing a regional Asia Pacific digital agreement, at least initially, with like-minded countries.

Mr. PERRY. Well, I sure hope so. I agree with you. I think that the regional framework is what we are seeking. You just do not know if it is possible. And I am just wondering if the individual agreements, where you get started with something, would set the tone for a regional framework even though you did it piece by piece by piece. It is not optimal, but at least we can get there.

So I appreciate your input.

Mr. Chairman, I yield back the balance.

Mr. BERA. Great. Thank you.

Let me now recognize the gentleman from California, Mr. Sherman, for 5 minutes of questioning.

Mr. SHERMAN. Thank you. And thank you, Mr. Chairman, for holding this hearing.

First, I want to emphasize that while there is a lot of support for rejoining TPP here in Washington, TPP is DOA with the American people. We saw this in 2016, where every Presidential candidate opposed TPP, and the people voted for the Presidential candidate who seemed most passionate in his opposition. In 2020, no Presidential candidate thought that they could sell TPP to the American people.

So we should be focusing here, and I think we are focusing here, on specific agreements dealing with digital because the American people probably cannot be convinced that goods made at 35 cents an hour in Vietnam should have free access to the U.S. market over the dead bodies of the labor leaders killed by that regime.

When we focus on China, they have tremendous power in our government and in our society because of the economic relationship, but it is not reciprocal. There are no lobbyists in Beijing working for trading partners of American companies or American companies themselves influencing Chinese policy. But the power that China has over Congress, because of its economic relationships, is enormous.

For that reason, we rarely even threaten the much higher tariffs that would need to be threatened to eliminate what is the largest and most pernicious trade deficit in the history of the world.

When we focus on digital, one important aspect of that is entertainment, and we have seen the power of the Chinese Government. As NBA stars fawn over each other as to who can apologize most for how the Uyghurs are treated, or in my own city, in Hollywood, where studios know that they will not have access to the Chinese markets if they ever make a movie about Tibet.

Scathing reports have been issued by the global Federation of Labor, the ITUC, and the global service sector labor federation, PSI. And without objection, I would like to enter both of these reports into the record.

They raise the issue of whether, through these international treaties, big tech can handcuff Congress before we can regulate them, before we can deal with monopolistic abuses, and can lock in a regulatory scheme favorable to themselves which Congress cannot change without the permission of dozens of other countries.

But I want to focus also on financial services. As you know, I chair the Capital Market Subcommittee. There we saw Morgan Stanley, in effect, forced to recommend that its customers buy more Chinese stock in order to get access to the Chinese market. But I want it to focus on one particular aspect of this.

Ms. Bliss, we have got to ensure that financial services firms are protected from the threat of forced data localization. That is one area where we have bipartisan agreement, both in the industry and from U.S. leadership.

Do you agree that the Biden Administration should build on that foundation against this effort by many countries, but especially China, to say, Oh, the data has to be kept in that country so that then oppressive governments can have access to that data to oppress their people?

How should the Biden Administration prevent these data localization initiatives?

Ms. BLISS. Thank you, Congressman Sherman.

And you really hit on what is one of our top digital priorities. We believe that data localization is pernicious, unjustified, and that I think the U.S. itself has worked out ways to ensure that regulators can get the information that they need, and if they cannot, they can resort to data localization, looking at the precedent that we have set on financial services in the USMCA financial services chapter.

So we think that that is a good balance, and a good way to combat.

But I absolutely agree that the elimination of data localization continues to be a major priority in the Indo-Pacific where it is, unfortunately, a continuing problem. Even among allies like Korea, Indonesia, Vietnam, it is a huge problem. And so, I think prohibiting data localization has to be a continuing priority, no question.

And let me also say——

Mr. SHERMAN. I would just also comment the regime in Ho Chi Minh City and Hanoi is not an ally of the United States. And I look forward to a more formal regulatory dialog with China, as we have with the U.K. and, again, India on these digital issues.

And I yield back.

Mr. BERA. Great. Thank you.

Let me now recognize the gentlelady from Missouri for 5 minutes of questioning, Mrs. Wagner.

Mrs. WAGNER. Yes. I thank you, Mr. Chairman, and I want to thank our witnesses certainly for their time and expertise.

As co-chair of the ASEAN Caucus, I am glad that this committee is examining the critical importance of trade and economic ties in the Indo-Pacific. China is determined to expand its influence throughout the region by subverting, replacing, or blocking the global rules and norms that the United States has championed for decades. Our partners in Southeast Asia are being increasingly targeted by China and are just absolutely desperate for the United States to show leadership and commitment.

Sadly, this Administration has neglected to offer, I think, a robust and specific plan to deepen U.S. economic engagement in the region.

The United States should be laying out a clear, a concrete, and a detailed roadmap for expanding economic and trade ties with Southeast Asia. My Southeast Asia Strategy Act, which I am proud to say was signed into law December 27th of 2021, will require the Administration to do just that.

China wants to rewrite global economic rules, especially in the digital economy and other emergent sectors. The United States must be proactive in shoring up existing international standards and building out the foundational agreements for the economies of the future.

This is why I was pleased to join Representatives Bera and Chabot in calling on the Administration to immediately begin negotiating a digital trade agreement for the Indo-Pacific. Vague promises to, quote, "explore an economic framework for the Indo-Pacific" will simply not be enough. China has already taken a number of actions to exert control over the development of digital trade rules, including by convening the PRC-led Regional Comprehensive Economic Partnership, or RCEP.

RCEP includes extremely concerning digital policy provisions that benefit China's authoritarian model of digital regulation. I worry that if the United States allows RCEP to form the basis for international digital standards, there will be serious ramifications, especially for human rights.

Ms. Bliss, how do RCEP digital provisions advantage authoritarian governments and help dictators restrict free speech and target vulnerable groups?

Ms. BLISS. Thank you, Congresswoman. And thank you for the work on—as you co-chair the ASEAN Caucus and also for the legislation——

Mr. BERA. Ms. Bliss, I would have you turn your camera on.

Mrs. WAGNER. Your camera is off.

Ms. BLISS. Sorry. Now it is on. Thank you.

So thank you for your work in this area. I think it is extremely important.

And I think that it is critically important that the Administration, as you say, come out with a concrete plan. And I think our view would be that there are significant provisions that need to be added, and we need to not only—we need to build on USMCA and the agreement we negotiated with Japan on digital——

Mrs. WAGNER. Now, let me just say that I am concerned about this Regional Comprehensive Economic Partnership that is PRC-led.

Ms. BLISS. Yes. No, I was going to get to that.

Mrs. WAGNER. I have very limited time and more questions, please.

Ms. BLISS. Right. So on RCEP, the way that it is so concerning is that there are flexibilities built in so that members of RCEP cannot observe various disciplines to the data localization provisions——

Mrs. WAGNER. Thank you, Ms. Bliss. Thank you. I am going to reclaim my time here.

Let me ask another question. It is very clear that China also hopes to use digital rulemaking to insulate itself from sanctions and other economic consequences of their human rights abuses and violations of international laws.

Ms. Bliss, if the United States does not take swift action to negotiate digital trade agreements, how might the PRC use digital rules to weaken our sanctions regime?

How do we prevent this?

Ms. BLISS. Well, again, if we do not get involved, I think, fortunately, there are other nations who are building a network that we are, unfortunately, outside of and will not benefit from. But I think that the PRC is being successful, both in terms of trying to extend its influence through—by joining CPTPP and also DEPA. And so, I think that is a threat that we need to face.

And, so, to your question, as I understand it, it is how can—what kind of a threat does China really pose? And I think it is through the potential of joining CPTPP, DEPA, as well as its ongoing activities multilaterally.

Mrs. WAGNER. OK. Thank you.

My time has expired. I appreciate the chairman's indulgence. And, Mr. Chairman, I have some other questions I will submit for the record, and I thank you very, very much.

Mr. BERA. Thank you, Mrs. Wagner.

Let me now recognize the gentleman from California, Mr. Lieu, for 5 minutes.

Mr. LIEU. Thank you, Chairman Bera, for holding this important hearing.

My question goes to Mr. Feith. The problems you identified seems to go more toward the fact that you have authoritarian countries versus free and open societies like the United States. So one reason that Russia was able to successfully execute, as our Department of Justice found, a sweeping and systematic attack of U.S. elections in 2016, is because in the U.S., we do not censor what people post on Twitter or Facebook.

The fact that China can do all sorts of things to software companies and other businesses in China is very different than in the U.S., where our own U.S. Supreme Court has made it difficult to even patent a number of kinds of software.

So when we have a free and open society, how is it that if we do any of these trade agreements, it will affect any of the concerns that you identified in your testimony? I am just curious how that would address the harms that you put out.

Mr. FEITH. Yes. Thanks for the question.

I think, of course, the difference that you point out, you know, that is so fundamental between free and open society and the authoritarian society is enormous. And I think that there are areas where the problems of nonreciprocal trade and nonreciprocal digital trade and data exchange, essentially they are areas where we wouldn't be able to pursue remedies, and we wouldn't want to pursue remedies for the reasons that you say. If a reciprocal remedy is to try, you know, set up in America a censorship regime that looks like China, that is not appealing.

But there are many other areas where I think, you know, an approach of a pursuit of a degree of reciprocity would be entirely consistent still with the free and open society at home, would be beneficial for national security interests around things like the protection of sensitive personal medical or genomic data, access to sensitive types of laboratories, corporate or academic, access to other sensitive sectors. And I think that some of these could be affected, you know, reformed, and approved by U.S. regulation or law in a fashion that is entirely consistent with remaining a free and open society here.

Mr. LIEU. So what we are talking about is not any digital trade agreement with China? Right? It is with other countries? So I am still trying to understand how this would sort of address the harms that you say are emanating from countries like China?

Mr. FEITH. Oh, absolutely. My point was that there are certain benefits to derive from a digital trade agreement in the Indo-Pacific, but they are largely separate from the additional very important digital trade-related tasks of beginning to scrutinize and then selectively restrict some of the types of data exchange that we have with China. We wouldn't do that through a digital trade agreement with China. We would do that through mechanisms like this new

ICTS regime, which is an interagency regime led by the Commerce Department, or you could do it through some of the legislative proposals that have emerged on the Hill.

But, no, the idea is not that that would be done through a trade agreement.

Mr. LIEU. All right. So I am a recovering computer science major, and I see how quickly technology moves. I believe it is impossible to stop technology. At most, we might go to regulated at its edges.

Just look at TikTok. Try to ban it, like, good luck with that; right. We saw what happened.

With Uber, what we saw happen is largely, my view is Uber broke a bunch of laws at the very beginning, but they went ahead and just did it. People liked the service, and now people use it.

And so when digital technology moves that quickly, I have concerns about any sorts of regulation from Congress or treaties where it would be very hard to change if we get it wrong.

Now, having said that, I do know we do have digital-free trade agreements with Australia, with Japan, with South Korea, with a number of other countries. So my question is, why do not we just do that? What if we simply went to Singapore and said, Hey, why do not we do a digital-free trade agreement? Indonesia, why do not we do that? Or in New Zealand, and so on. Why not just do it country by country?

And that is for any member of the panel.

Ms. CUTLER. Perhaps I can just respond.

I just think doing these types of agreements bilaterally doesn't produce the same kind of impactful result that you will get from working with a whole group of countries. And by getting a group of countries to agree to common rules, common standards, and common norms, it is much more impactful and, frankly, develops kind of a collective reaffirmation of the types of democratic principles and values that, you know, we are advocating.

So, again, you can do it bilaterally, but I am not sure why you would want to.

Mr. LIEU. Thank you.

Ms. BLISS. If I could quickly jump in——

Mr. BERA. The gentleman's time has expired.

Let me go ahead and recognize the gentleman from Tennessee, Mr. Burchett, for 5 minutes of questioning.

I think you are on mute.

Mr. BURCHETT. I was making a play for bipartisanship. I was going to say—ask Ted Lieu if he would stay on for a minute and let her finish answering. She wanted to answer that question, and I was curious about that myself. If you'll go—and I will yield my time to do that. Just take a little bit because I am going to cut you off.

Mrs. KIM OF CALIFORNIA. Mr. Chairman, was I recognized? I apologize.

Mr. BERA. No. Mr. Burchett.

I think Mr. Burchett is allowing you time to answer that question.

Ms. BLISS. Well, you are very kind, Congressman. Thank you.

Just very quickly, two points: One is—and I think this came out in Congressman Lieu's question, but also in a previous question

that was posed, and that is that all of U.S. trade agreements enshrine the principle of the right to regulate. And I think that is a very important point to make in terms of concerns about the degree to which a trade agreement can constrain what the U.S. Government can do legislatively or administratively. So that is point one.

And then point two, I just wanted to add that I think in terms of emerging technologies and how swiftly things are changing, an important point to make is one of the innovative provisions that the U.K. has included in its FTAs, which I think we ought to take a close look at as well, is a regulatory sandbox for digital regulation. And I think enshrining that and making that part of it is a good way of addressing the rapidly changing and evolving digital landscape.

Thank you.

Thank you again very much.

Mr. BURCHETT. Yes, ma'am.

I do not agree with Ted Lieu on much, but I wanted to hear what—he has been my buddy, so I wanted to make sure he got the answer on that.

What can be done to protect against the Chinese Communist Party gaining control over our undersea fiberoptic cables and over the data that flows through them? Anybody can answer that, please.

Mr. FEITH. I am happy to take that, sir.

On the undersea cables, I think broadly, somewhat crudely, there are perhaps three broad categories.

One is the question of whether we, as a U.S. Government, support undersea cables being built directly from our country to China. That is something that the FCC basically put an end to over the course of the last several years. They stopped issuing new landing licenses for cables of that kind I believe in very early 2017. And then in June 2020 or so, they undid a previously granted plan that would have connected Los Angeles to Hong Kong. That was the Pacific Light Cable Network, and they said they are not going to license that to turn on—to touch from London—or rather from Los Angeles to Hong Kong. It is only going to go from Los Angeles to Taiwan and the Philippines.

So the landing license that the FCC has authority over is one big one; but there are two other major areas of this that also would seem to relate to American data integrity and ally data integrity, which is to what extent Chinese companies, like the former Huawei subsidiary, HMM Tech, are welcome to build cables that if not touching the U.S. connects to other allies and partners of ours.

So, for example, HMM Tech actually just landed for the first time in France. I believe this may have been the first time they landed in a NATO country——

Mr. BURCHETT. I remember, but prior to that they were Huawei, right? They just changed their name to HMM. Is that pretty much the case?

Mr. FEITH. Huawei Marine was a subsidiary of the Huawei we all know.

Mr. BURCHETT. I get it. I get it, yes.

Mr. FEITH. It is a bit of a kind of a—yes, bit of a corporate shell game. But, yes, it is the same company. They build cables.

And so, I think there is a question, that is a question for us, about allied consultations and diplomacy, which is how much do we make it clear to our friends that we consider this a major data integrity risk when ally countries with whom we have sensitive, you know, communications might be inviting this Huawei affiliate into their critical telecommunications infrastructure to build new cables. And there is also the related matter of the maintenance of existing cables, where——

Mr. BURCHETT. OK. I am going to run out of time, but—hang on, David. I am going to run out of time. What can we do to stop that?

Mr. FEITH. Well, again, I think at home you have domestic licensing authorities which the FCC has been using. Diplomatically we can encourage friends, to include the French and others, to reconsider these sorts of landings. There are also—essentially there are authorities, you know, for example, like DFC Financing, and Eximbank Export Credit that allow the U.S., or even the Japanese and European competitors of these Chinese undersea cable firms to give certain bidders more competitive pricing because Huawei in classic Chinese fashion seeks to underbid and win contracts that way.

And I think all of those measures are things we should take very seriously as you are suggesting.

Mr. BURCHETT. All right.

Thank you, Mr. Chairman. Thank you for your indulgence. Appreciate it.

Mr. BERA. Thank you.

The chair now recognizes the gentlelady from Virginia, Ms. Spanberger, for 5 minutes of questioning.

Ms. SPANBERGER. Thank you very much, Mr. Chairman. And thanks for our witnesses being here.

I have long been concerned about China's growing influence as a leading supplier of 5G technology. Chinese control of this important telecom technology could threaten the privacy, the data, the security of American countries and certainly American consumers.

So last Congress, I was very proud to introduce and pass, with a vote of 413 to 3, legislation that would require the Administration to develop and plan a counter Chinese monopoly plan and trajectory for us in the 5G space.

And most recently, I was proud to cosponsor, vote for, and see signed into law the bipartisan Secure Equipment Act of 2021 to remove potentially harmful equipment from our Nation's communication networks.

So as sort of followup to this landscape of what we have done so far, I am curious, how could U.S. engagement with Indo-Pacific countries foster a more diverse, resilient, or secure telecommunications ecosystem that supports our domestic priorities while also expanding our engagement in the region?

And I will open it up to any of the witnesses who may want to speak to that, either in agreement or in disagreement with the premise of my question.

Ms. CUTLER. Well, I will start.

I am in total agreement with the premise of your question. The whole idea of working with our partners and allies in the Indo-Pacific is to kind of build that ecosystem that reflects, again, our val-

ues, our norms, our priorities, taking into account their concerns and priorities as well. But the more we can work with them and develop this ecosystem, it is not going to be static. It will continue to expand into other areas, particularly as technology develops.

So I think, you know, you are right on the mark with your question, and I think that is one of the important elements, and really the urgency now, of working with our countries to build that ecosystem.

Ms. SPANBERGER. In looking at building that ecosystem, are there any suggestions that you all—again, I will open this up to any of the witnesses—would make to members of this committee in terms of either legislatively or things we should be thinking about as we are looking toward our partners and potential increased partnerships in the Indo-Pacific?

Are there any things that you would point us to or things that you think we should be focusing on from a congressional standpoint?

Mr. FEITH. Congresswoman, I will take that quickly.

One thing the U.S. Government has learned in recent years, sometimes through difficulty and frustration, is that as we try to make our own policy and consult with our friends about policy on the sorts of telecommunications infrastructure matters that you have raised, there is sometimes a problem of an inability to address the full relevant technology stack.

And the previous question about undersea cables reflects that, where, you know, we had an explosion in interest over the last 5 years, let's say, in 5G where we basically ended up focusing our diplomacy aggressively and with some success, but quite narrowly, on the matter of terrestrial hardware, you know, which bay stations for terrestrial systems will our allies and partners install. And that is extremely important.

But all of the same concerns apply to undersea cables. All of the same concerns apply to data centers and the cloud. All of the same concerns apply throughout that process, and we, in our system and very much with allies and partners, we found in our diplomacy that often, unless we made a specific, you know, point, but actually the concern that is about terrestrial also relates to undersea, it also relates to cloud, our counterparts wouldn't naturally make the inference.

And I think as we do policy and legislating, we might fruitfully bear that in mind.

Ms. SPANBERGER. And, Mr. Feith, you mentioned multiple times the diplomatic engagement and, you know, through our diplomatic discussions. And so, I would just note that we do need to have a very strong diplomatic presence across Asia, so I am personally—and I think many of my colleagues share this concern that so many of our Ambassador positions across the region, especially in Southeast Asia have gone unfilled, in some cases, for years. And so I think that this—it certainly has an impact on our ability to cooperate on shared U.S. interests, to include putting a check on Chinese expansionism, but also bolstering public health in their response to COVID.

And so I wonder if you, in the closing moments that we have left, have any comments on that in terms of the necessity and value of having those positions filled?

Mr. FEITH. No. I would agree. It is extremely valuable, and the sooner the better.

Ms. SPANBERGER. Thank you.

Mr. Chairman, I yield back. Thank you very much for this hearing.

Mr. BERA. Great. Thank you.

Let me now recognize the gentleman from Kentucky, Mr. Barr, for 5 minutes of questioning.

Mr. BARR. Thank you, Mr. Chairman. Thank you to our witnesses for your testimony.

Let me especially thank Mr. Feith for what I think is the most salient point of this entire hearing, in his prepared testimony when he quoted General Secretary Xi Jinping in talking about data. And I will quote from Mr. Feith's testimony what the Chinese leader said. Quote, "the vast ocean of data, just like oil resources during industrialization, contains immense productive power and opportunities. Whoever controls big data technologies will control the resources for development and have the upper hand."

Make no mistake, that is the modus operandi of the Chinese Communist Party.

Beijing, indeed, recognizes that competition for global influence in the 21st century will require harnessing this data, dominating this data to achieve commercial, technological, military, and intelligence advantages.

That is what it is doing. I want to flag that testimony. I want to highlight it. I want to underline it. That is what this hearing is all about, and we need to compete and we need to counter that threat.

So, Mr. Feith, in response to that—and also I would invite our other witnesses to chime in here—tell us about the extent to which the Chinese-led Regional Comprehensive Economic Partnership is enabling China to obtain those advantages in data, and amplify whatever other threats RCEP poses to the rest.

Mr. FEITH. Well, thanks, Congressman. I appreciate your comments about the testimony.

I will also happily defer on a lot of the RCEP details to my colleagues, you know, with USGR experience who are deeper on this.

I would just say briefly, I think what RCEP does with respect to allowing China to continue to carry out this aggressive and mercantilist and predatory data strategy is mostly failing to check any of that in the Chinese system, which is to say that the rules in RCEP that relate to data, cross-border data flows, data localization are soft. They are, in some cases, I think non—kind of unenforceable because they are not subject to the mechanisms that do exist in that agreement.

What makes it low standard is it basically allows governments to do as they please. And in the case of Beijing, doing as they please is the construction of this intensely controlled posture where, frankly, Beijing is succeeding at hoarding all of its own data and seeking to absorb all of the rest of the world's data through means either legal or illegal. And I think that is the challenge that

it poses to us in recognition that we have national security concerns with the exposure of our data, and we all have intense competitive concerns with the control of data over time as an input into innovation and technology.

Mr. BARR. Ms. Bliss, could you also offer your thoughts on that and particularly what threats RCEP poses, and what changes to the digital trade landscape in the Asia Pacific and the Indo-Pacific region going forward?

Ms. BLISS. Yes. Well, I would largely agree with Mr. Feith's comments with respect to the weaknesses and the dangers of RCEP.

And as I have previously said, I think, overall, the flexibilities that are built in in the agreement in terms of allowing a country, a member like China, to do as it pleases and impose its own policies is a real danger and risk to us.

As Mr. Feith mentioned, the data localization and cross border flow provisions are incredibly weak and ineffective, and the fact that you have these kinds of standards in the ASEAN region with the significant GDP that it represents is extremely problematic.

Mr. BARR. Reclaiming my time in the final time.

Obviously, the Trump Administration pulled out of TPP. The Biden Administration is signaling a lack of interest in CPTPP. How do we prevent China from being part of that?

Ms. BLISS. Well, I do not know if you are addressing it to all of us. I can start maybe just by saying I think China will have real hurdles, and it is of great concern that they have applied to join CPTPP. The good thing, however, is that the existing CPTPP partners have to agree on the application and on—China would have to agree to the conditions that were put on the terms of its accession and the negotiation that it would have to go through.

So working with our allies, I think they would share our concerns, and I think there would be real questions as to whether China could actually meet the standards necessary to join CPTPP. But it is not a given, so it is an ongoing concern. But I do think the fact that that mechanism is in place, where you do have to get agreement in order to accede and go through negotiation, is at least a safeguard that is in place.

Ms. CUTLER. If I can just add, though, I think we need to take this—and this is in my testimony—very seriously, and just relying on our allies and partners to kind of block even the establishment of a working party to start those negotiations for China CPTPP accession, we cannot count on them. We are not in that agreement. We cannot block it. And even our allies and partners, guess who their largest trading partner is? It is China, where are their supply chains, you know, where they strengthen their supply chains and increasing their economic integration.

And so, while it is important behind the scenes that we work with our allies and partners, there is nothing better that we can do than by getting back in the region economically, sharing our affirmative agenda, and getting others to sign on, and really lead the economic future of the Indo-Pacific.

Mr. BARR. I agree with you, Ms. Cutler.

My time is expired, and I yield back.

Mr. BERA. Let me now recognize the gentleman from Virginia, Mr. Connolly, for 5 minutes of questioning.

Mr. CONNOLLY. Thank you so much, Mr. Chairman, and thank you for having this hearing.

Ms. Cutler, was the whole issue of digital services and digital governance addressed in the TPP?

Ms. CUTLER. Clearly, parts of it were, but, frankly, that chapter is pretty outdated now. I mean, it was negotiated probably 10 years ago now, put into force 3 years ago. And so, you know, it would be significant updating——

Mr. BERA. Mr. Barr, you have to mute yourself.

Mr. CONNOLLY. I would ask that my time be paused, Mr. Chairman.

Ms. CUTLER. I think I answered your question, so——

Mr. CONNOLLY. So I guess I want to get at, when the United States walked away from its own treaty that it had written, it had negotiated, the TPP, when Donald Trump decided to walk away from that, did that create a vacuum in terms of economic relationships in the broader Trans Asia Pacific region?

Ms. CUTLER. Well, it absolutely created a vacuum. And, you know, our trading partners, they got their act together to go forward with the CPTPP without us. Now, lucky for us, they kept most of the provisions intact. But as they go forward and China becomes, you know, increasingly interested in a lot of these arrangements, their ability and their interests in just pursuing what we want them to pursue, you know, is something we just cannot count on.

Mr. CONNOLLY. And it also created a vacuum, did it not, that China is actively filling?

Ms. CUTLER. Absolutely. I mean, the fact that the irony of all ironies is China applying to join the CPTPP.

Mr. CONNOLLY. Yes.

Ms. CUTLER. Whoever thought that, you know, that wasn't in the cards.

Mr. CONNOLLY. I mean to me, this was one of the most self-inflicted wounds any great power could ever administer to itself.

So here we have, you know, something like 40 percent of the world's GDP agreeing to enter into, you know, this regime that promoted liberal economic trade and investment and intellectual property protection, human rights, environmental standards, labor standards for the first time under the American protective channel. And we walk away from our own treaty, and that leaves those countries that were willing to partner with the United States sort of at the mercy now of, you know, outrageous fortune and the Chinese.

What is a country like, for example, Vietnam to do absent the protective umbrella TPP would have provided?

And are you seeing, as a consequence of that subsequently, countries either in tandem or individually cutting their own deals with China as best they can?

Ms. CUTLER. Well, I think RCEP is the testament to that. As long as the TPP negotiations were going on, frankly, there was a lack of interest in the RCEP negotiations. But the fact that 15 Asian countries came together, including seven CPTPP members, and concluded RCEP that was brought into force earlier this month

without us is really a testament to not only the vacuum we created, but their intent and their confidence to go forward without us.

Mr. CONNOLLY. You know, there were a lot of criticisms, especially, frankly, in my coalition, my Democratic coalition, about TPP and it did not meet the standards that we wanted. Does the Chinese agreement have human rights standards as part of the agreement?

Ms. CUTLER. I mean, RCEP is really just—the chapters are a subset of CPTPP. It does not include human rights, does not include State-owned enterprises, does not include labor, does not include environment, and the list goes on.

Mr. CONNOLLY. Ah. So while there were people who found TPP not entirely adequate, or not everything they wanted, what has replaced it has zero of that?

Ms. CUTLER. RCEP does, but let's keep in mind there is, you know, CPTPP——

Mr. CONNOLLY. No, no. I am only talking about RCEP now.

Ms. CUTLER. Yes, correct.

Mr. CONNOLLY. And I just think that is the threat. OK. Making perfect through the enemy of the grid has now hugely increased China's influence to the very region we were trying to counter it, and diminished our own because we walked away from our own agreement. And, oh, by the way, ironically, the standards you thought were inadequate are nonexistent under the Chinese umbrella.

Ms. CUTLER. And RCEP also is not a static agreement. It provides committees. It has a work program. And new rules will probably be discussed among the 15 countries going forward.

Mr. CONNOLLY. Thank you so much.

Thank you, Mr. Chairman.

Mr. BERA. Thank you.

Let me now recognize the gentlelady from California, Mrs. Kim, for 5 minutes of questioning.

Mrs. KIM OF CALIFORNIA. Thank you, Chairman Bera, and thank you, Ranking Member Chabot. And I want to thank all of our witnesses for joining us today, and, especially, Ms. Wendy Cutler. It is really good to see you.

Leveraging U.S. engagement in the Indo-Pacific on digital economic opportunities is crucial toward securing U.S. national interest in the region and opening new doors for American commerce.

So in my time in Congress so far, I have strongly urged the Biden Administration many times to pursue trade agreements that would implement new rules on cross-border data flows, restrictions on data localization, and protection of source code.

Ensuring the secure movement of data across borders with countries that maintain similarly strong standards is critical toward promoting future digital trade that will bolster global commerce and boost technological innovation.

As the world continues to evolve in the digital age, it is imperative that our policies and partnerships evolve with it, and that the U.S. is at the end of countering the technical authoritarianism and democratizing visual technologists.

For these reasons, I led a letter with our fellow Members of Congress to the Biden Administration last November urging the Presi-

dent to reengage the Indo-Pacific on digital trade through new or updated bilateral, and plurilateral trade agreements. However, I have yet to see a response to my letter from President Biden, and this committee has yet to see any substantive action in the Indo-Pacific on pursuing new digital trade opportunities.

So let me ask my first question to you, Mr. Feith. I would like to focus my questioning first on China's Digital Silk Road. Can you provide insight into the present challenges this poses to U.S. national security and economic interest in the Indo-Pacific? And what are potential responses Congress and the Administration can take to counter these challenges?

Mr. FEITH. Sure. Thank you for that.

Well, so, the Digital Silk Road of China is essentially the digital component of the broader Belts and Road Initiative, or One Belt One Road strategy as the Chinese still say it in Chinese.

And essentially there has been, I think, a lot of attention, justified attention on Chinese-built projects like ports that have themselves allowed Chinese military access or caused debt problems for the countries that received them. But actually the Digital Silk Road, which is to say the digital telecommunications infrastructure that is largely invisible, you know, harder to take a picture of than a port, is probably the more pernicious threat, as I think your question suggests.

And perhaps—in brief, but the threats are two main types. One is simply to the data integrity, which is to say that when Chinese companies that are instruments of the State and are subject to coercion by the Chinese State are building undersea cables or, you know, mobile telephone infrastructure, infrastructure for, you know, commerce and government business in these third countries, all of that is subject to compromise by the Chinese State or by the Chinese security services. And that is a very big problem for the data integrity. And there is the related problem of the political influence that comes with it.

These Chinese overseas infrastructure projects seem very often designed to basically insinuate the Chinese Communist Party into the local politics of these countries as a way of exerting some very effective long arm influence, and sometimes that is collecting information and——

Mrs. KIM OF CALIFORNIA. Thank you, Mr. Feith. Yes, thank you. Thank you for your answer.

In the interests of time, I would like to ask Ms. Cutler a couple of questions. Actually, I will just throw that all in there.

What existing or potential future agreements offer the best frameworks for personally digital trade opportunities with the Indo-Pacific region? And what strategies do you realistically believe this Administration will pursue? And which countries will they primarily seek to partner with?

And then if you can further provide the insight on opportunities that remain out there for a partnership with ASEAN member nations.

Ms. CUTLER. Well, thank you very much, Congressman Kim, and it is great to see you.

Just in short, the Administration is soon to unveil its Indo-Pacific economic framework with details in all of the areas that they

have listed, including digital standards and digital technologies. So I am expecting that we are all going to see a lot more very soon, which will include some kind of initiative on digital with our partners in the region.

Now, when we talk about which partners, they are kind of the usual suspects, Australia, Japan, New Zealand, Korea, Singapore. But from my perspective, for any digital initiative, even for the overall framework to be effective, it needs to go broader than that, particularly with respect to including countries from Southeast Asia. And if that means there needs to be certain flexibilities to allow certain countries to sign on to certain obligations from the git-go, and then over time to phase in others, I think that is, you know, a worthwhile approach.

So I think we will be seeing more digital very soon. I know both USTR and Commerce are working very hard to kind of build out that agenda, and there is a recognition that this is, you know, an important part of the overall framework.

Mrs. KIM OF CALIFORNIA. Thank you.

Thank you for allowing us to go over time, Chairman. I yield back.

Thank you, Ms. Wendy Cutler.

Mr. BERA. Thank you.

Let me recognize the gentlelady from North Carolina, Ms. Manning, for 5 minutes of questioning.

Ms. MANNING. Thank you. Thank you, Chairman Bera and Ranking Member Chabot, for organizing this very important hearing. Thank you to our witnesses for sharing your expertise with us today.

I would like to echo Representative Spanberger's concerns about the lack of envoys who have been confirmed throughout the region and, frankly, throughout the world, and how that is hampering our efforts and our ability to achieve trade agreements and other important agreements in this region and around the world. And many of those envoys and Ambassadors are awaiting confirmation in the Senate, and I think it is causing real harm to this country.

I would also like to pick up on the issue that Representative Connolly raised, and that is the serious error that the Trump Administration made in walking away from the TPP, an agreement that we forged to create a significant regional alliance that would have been hugely beneficial to the U.S. in terms of trade and influence on the standards and behaviors in the region.

And right now, as we are talking about all of these agreements that we have seen created between other countries in the region, we are basically being left out and we are being forced to play catchup.

So, Ms. Cutler, you mentioned a little bit what you would hope to see is the Biden Administration release its Indo-Pacific economic framework. I wonder if you could talk a little bit more about what you would like to see to reinforce our efforts to create a regional block that is more in line with our values and priorities.

Ms. CUTLER. Yes. I mean, what I would like to see are just details in all of these areas which show that this initiative overall is serious, that we are committed to the long term to economic ties with the region, and that it goes beyond just principles and best

practices. It actually has rules, norms, and standards that we will be asking others to join us in embracing, and have some real tangible outcomes that really matter and are impactful.

So whether it be in digital or in infrastructure or in clean technologies or supply chains, there is a lot to be done in all of these areas and, frankly, you know, we need to move quickly.

Ms. MANNING. Thank you.

Ms. Bliss, since President Trump withdrew from the TPP in 2017, and in the absence of any substitute engagement, can you talk to us about what the impact has been on U.S. companies in the region? In particular, what kinds of discriminatory trade barriers have we watched in the digital realm in the past few years?

Ms. BLISS. Thank you, Congresswoman.

What we have seen in particular is a continued rise in digital protectionism, and as I mentioned previously, particularly in the area of data localization requirements, and on restrictions on cross-border data flows, I can mention specifically—I mentioned Korea and Indonesia in particular as examples of where data localization measures are still significant problems for U.S. companies across the services sector. And so that, I believe, in part, is a direct result of the U.S. not participating and being able to be part of the TPP, and now CPTPP.

But I will say, as previous witnesses have said, I would totally agree that, you know, we have gone beyond CPTPP and what we included in digital trade in USMCA, the U.S.-Japan agreement but, more importantly, I think what some of our trading partners are doing, Australia, Singapore, and the U.K. in particular, and there is some really strong innovative conditions that I think can be helpful in combating the rise of digital protectionism.

So I think we need to look at those.

Ms. MANNING. Thank you.

Mr. Feith, we have seen how China exerts pressure against American companies, like Apple, forcing them to store consumer data on Chinese servers, orcensor applications in return for market access.

What can the U.S. do in our trade engagements to push back on these efforts across the region?

Mr. FEITH. It is a—frankly, it is a very difficult one in the sense that, you know, there are certainly some companies—and Apple is a real example—that have made themselves very strongly dependent on what they can get only in China, in Apple's case in terms of the manufacturing supply chain and, therefore, they are in a position where they comply with even the very onerous and predatal or even fundamentally unfair and nonreciprocal laws and regulations that China imposes.

I think that, you know, the ability to fix that, frankly, from Washington is limited, which I think is why the problem persists to such an unfortunate degree.

I think in the long term, though, this digital and data trade discussion, you know, might need to point, you know, frankly, into a kind of a world that we feel like we cannot even really imagine at the moment, where essentially we have arrangements where countries that want to follow essentially, you know, democratic and liberal norms of data trade align ourselves into, you know, something

of a data trade zone and a block, and actually consider over time, not only privileging each other, but actually imposing restrictions and tariffs on the likes of China and others who will continue to not follow these rules of, you know, reciprocal and open trade.

Ms. MANNING. Thank you.

My time has expired, and I yield back.

Mr. BERA. Thank you.

I want to thank our members for their questions and to the witnesses for their responses.

With member questions now concluded, I will move to my closing remarks and then recognize the ranking member for any closing remarks that he may have.

I think, you know, for folks that are watching this, as well as for our witnesses and members of the Administration, you've seen bipartisan support for engagement and, you know, a desire from the members of this subcommittee, but I believe in a bipartisan-bicameral way, a desire for the United States to engage with the region in a way that, you know, doesn't disadvantage our workers, addresses environmental concerns, but also sets standards and norms for digital trade and, you know, beyond in the region.

I think recent history also suggests, you know, with USMCA that with an inclusive process that does take time, does take a lot of effort, you can come up with a strong bipartisan agreement that it can be supported by labor, environmental groups, the business community, and others and has a strong standard.

So I welcome the ability to work with the various groups, but also with the Administration as they engage and start to lay out their economic framework for engagement with the Indo-Pacific. And I look forward to working with the ranking member, Mr. Chabot, and other members of this subcommittee as this process goes forward.

And with that, let me go ahead and recognize the ranking member, Mr. Chabot, for any closing comments that he may have.

Mr. CHABOT. Thank you, Mr. Chairman. And let me commend you for holding a really excellent hearing, I believe, on a very important issue.

As I said in my opening statement, countries throughout the Indo-Pacific are hungry for U.S. economic engagement. And I agree with you that the digital trade is a good place to start. Such an agreement would bring many benefits to the U.S. economy. And as the past chairman of the House Small Business Committee, I particularly appreciate Ms. Bliss mentioning the importance of a digital agreement for small-and medium-sized enterprises. The stakes are high if we sit on the sidelines.

As our witnesses have said, the PRC is seeking to export digital standards to the rest of the world that are radically different from those that we would create. Unfortunately, this Administration's rather nebulous statements about an economic framework for the region really do not inspire a great deal of confidence that their strategy is up to the task.

So I appreciate your leadership on this issue and look forward to working with you and our colleagues over on the Ways and Means Committee to make some progress on this critical area.

And with that, I yield back.

Mr. BERA. Thank you.

And I want to once again thank our witnesses and the members who participated in this very important virtual hearing.

And with that, the hearing is adjourned. Virtual gavel banging.

[Whereupon, at 12:04 p.m., the subcommittee was adjourned.]

APPENDIX

SUBCOMMITTEE HEARING NOTICE
COMMITTEE ON FOREIGN AFFAIRS
U.S. HOUSE OF REPRESENTATIVES
WASHINGTON, DC 20515-6128

Subcommittee on Asia, the Pacific, Central Asia, and Nonproliferation

Ami Bera (D-CA), Chair

January 18, 2022

TO: MEMBERS OF THE COMMITTEE ON FOREIGN AFFAIRS

You are respectfully requested to attend an OPEN hearing of the Committee on Foreign Affairs, to be held virtually by the Subcommittee on Asia, the Pacific, Central Asia, and Nonproliferation via Cisco WebEx (and available by live webcast on the Committee website at https://foreignaffairs.house.gov/):

DATE: Wednesday, January 19, 2022

TIME: 10:00 a.m., EST

SUBJECT: Strategic Importance of Digital Economic Engagement in the Indo-Pacific

WITNESS: Ms. Christine Bliss
President
Coalition of Services Industry

Ms. Wendy S. Cutler
Vice President
Asia Society Policy Institute

Mr. David Feith
Adjunct Senior Fellow
Indo-Pacific Security Program
Center for a New American Security

By Direction of the Chair

To fill out this form online: Either use the tab key to travel through each field or mouse click each line or within blue box. Type in information.

COMMITTEE ON FOREIGN AFFAIRS

Note: Red boxes with red type will NOT print.

MINUTES OF SUBCOMMITTEE ON *Asia, the Pacific, Central Asia, and Nonproliferation* HEARING

Day *Wednesday* Date *January 19, 2022* Room *Cisco WebEx*

Starting Time *10:08am* Ending Time *12:04pm*

Recesses *0* (to) (to) (to) (to) (to) (to)

Presiding Member(s)

Chair Ami Bera

Check all of the following that apply:

Open Session ☑
Executive (closed) Session ☑
Televised ☑

Electronically Recorded (taped) ☑
Stenographic Record ☑

To select a box, mouse click it, or tab to it and use the enter key to select. Another click on the same box will deselect it.

TITLE OF HEARING:

"The Strategic Importance of Digital Economic Engagement in the Indo-Pacific"

SUBCOMMITTEE MEMBERS PRESENT:

Chair Bera, Ranking Member Chabot, Rep. Sherman, A. Levin, Connolly, Lieu, Manning, Wagner, Perry, Buck, Burchett, Barr, Y. Kim

NON-SUBCOMMITTEE MEMBERS PRESENT: *(Mark with an * if they are not members of full committee.)*

HEARING WITNESSES: Same as meeting notice attached? Yes ☐ No ☐
(If "no", please list below and include title, agency, department, or organization.)

Yes

STATEMENTS FOR THE RECORD: *(List any statements submitted for the record.)*

IFR - Sherman (2)
SFR, Connolly
QFR - Titus
QFR, Wagner

TIME SCHEDULED TO RECONVENE
or
TIME ADJOURNED *12:04 pm*

Clear Form

Note: If listing additional witnesses not included on hearing notice, be sure to include title, agency, etc.

Subcommittee Staff Associate

WHEN COMPLETED: Please print for subcommittee staff director's signature and make at least one copy of the signed form. A signed copy is to be included with the hearing/markup transcript when ready for printing along with a copy of the final meeting notice (both will go into the appendix). The signed original, with a copy of the final meeting notice attached, goes to full committee. An electronic copy of this PDF file may be saved to your hearing folder, if desired.

HOUSE COMMITTEE ON FOREIGN AFFAIRS

SUBCOMMITTEE ON ASIA, THE PACIFIC, CENTRAL ASIA, AND NONPROLIFERATION

ATTENDANCE

PRESENT	*MEMBER*
X	Ami Bera, CA
X	Brad Sherman, CA
	Dina Titus, NV
X	Andy Levin, MI
	Chrissy Houlahan, PA
	Andy Kim, NJ
X	Gerald E. Connolly, VA
X	Ted Lieu, CA
	Abigail Spanberger, VA
X	Kathy Manning, NC

PRESENT	*MEMBER*
X	Steve Chabot, OH
X	Scott Perry, PA
X	Ann Wagner, MO
X	Ken Buck, CO
X	Tim Burchett, TN
	Mark Green, TN
X	Andy Barr, KY
X	Young Kim, CA

STATEMENT FOR THE RECORD CONNOLLY

Statement for the Record from Representative Gerry Connolly
"Strategic Importance of Digital Economic Engagement with the Indo-Pacific"
House Foreign Affairs Subcommittee on Asia, the Pacific, and Nonproliferation
January 19, 2022

As the fastest growing region in the world, the Indo-Pacific accounts for 60 percent of the world's economy and two-thirds of all economic growth over the last five years.[1] A study released in the fall of 2019 found that in Southeast Asia, 70% of the population is online and the region's internet economy expanded 5% between 2019 and 2020.[2] Home to many of the world's largest economies, the Indo-Pacific represents a unique opportunity for the United States to develop a framework that promotes U.S. digital industry and establishes a rules-based architecture that neutralizes the PRC's predatory economic influence in the region.

If trends are any indication, digital trade will continue to play an integral role in our economy for years to come, and a framework that opens up potential U.S. investment in the Indo-Pacific will benefit the U.S. economy. In 2019, the digital economy accounted for 9.6 percent of U.S. gross domestic product (GDP), supporting 7.7 million jobs in the United States.[3] From 2005 to 2019, real value added for the U.S. digital economy grew at an annual rate of 5.2 percent per year, outpacing U.S. economic growth by 3 percent.[4] One in four jobs in Fairfax County, located in Virginia's 11th district, are related to the 8,700 technology-focused enterprises located in Fairfax County, making it the third largest metro area for technology employment.[5] Some estimates indicate more than 60 percent of all U.S. service exports now have the potential to be delivered digitally to customers abroad.[6] During the global Covid-19 pandemic, digital trade has undoubtably grown to keep cross-border trade operational, providing a lifeline to economies worldwide when traditional trade means were constrained.

Digital trade is, by nature, different than conventional trade. Digital products and services are not often-times physically shipped across borders. For example, a consumer in another country can purchase an American online product or service and download it from the internet. With that said, a lack of commonsense trade rules and data localization requirements create trade barriers that stymie U.S. companies from expanding exports in the Indo-Pacific, while other countries, like China, actively create a framework that suits their own strategic interests.[7]

Expanding economic ties with the Indo-Pacific, especially in the areas of digital trade and e-commerce, is not only an economic priority for the United States; it is in our country's strategic interest. The United States previously had an opportunity to set the rules for digital economic engagement in the Asia-Pacific, where we already maintained longstanding commitments, with the Trans-Pacific Partnership (TPP). Our withdrawal from TPP and from the Indo-Pacific region in general under the Trump administration created a vacuum that provided an unbelievable gift to the government of China by eliminating our chances to negotiate a digital trade component within the greater agreement. They are still drinking champagne in Beijing.

---

[1] State Department Fact Sheet, "Secretary Blinken's Remarks on a Free and Open Indo-Pacific," December 13, 2021
[2] Reuters, "Southeast Asia's internet economy to cross $100 billion this year: industry report," November 9, 2020
[3] Congressional Research Service, "Digital Trade and U.S. Trade Policy," December 9, 2021
[4] ibid
[5] Fairfax County Economic Development Authority, "Paving the Way for the Future of Tech"
[6] John G. Murphy, "The Case for a Digital Trade Agreement," *U.S. Chamber of Commerce*, August 17, 2021
[7] USTR, "2021 National Trade Estimate Report on Foreign Trade Barriers," 2021.

In our absence, China has actively and successfully pursued a trade strategy in almost perfect harmony with its national security and strategic interests. Just a couple weeks ago, the Regional Comprehensive Economic Partnership (RCEP) entered into force for China and 10 other Asian countries that ratified the agreement. RCEP reflects a trade agreement with fewer commitments compared to the Trans-Pacific Partnership (TPP), though China has requested to accede to the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) the successor to TPP as well. Additionally, the PRC has requested to join the Digital Economic Partnership Agreement (DEPA) with Chile, New Zealand, and Singapore.

Countries in the Indo-Pacific region may prefer American digital products and services, but without a framework to lower barriers for American companies to enter the market, the U.S. will be asleep at the switch while the PRC expands their digital economic engagement in the Indo-Pacific through multilateral trade agreements, some of which the U.S. wrote and negotiated to forestall China's aggression. It is no secret that China uses its economic might as a means to pursue its strategic interests without regard to the proliferation of technology that allows governments to surveille their own citizens and restrict human rights and freedom of expression.

With that said, we cannot expect trade to be a panacea for the Asia-Pacific. Trade with the U.S. will not foster American-style democracies on day one of a free trade agreement. However, it will give U.S. companies and U.S. citizens access to markets that are partly closed off to U.S. goods and services. It will provide an alternative to China, a country that has used its trade ties to put smaller countries into a vulnerable, defensive crouch on matters such as maritime disputes. And, yes, trade with the U.S. will come with strings attached to allow for basic individual freedoms such as freedom of expression.

The United States has made commitments with a digital trade chapter in the US-Mexico-Canada Agreement (USMCA), as well as the U.S.-Japan Digital Trade Agreement, but they are not enough to exert global U.S. leadership on digital trade. In November, I was proud to join Chairman Bera and Ranking Member Chabot in sending a letter to U.S. Trade Representative Katherine Tai urging the Biden Administration to pursue such a digital trade agreement with partners in the Indo-Pacific.[8] A framework that establishes fair and transparent trading rules would naturally counteract China's aggressive and pernicious economic activity. Perhaps using a video conferencing software developed in the United States, Biden Administration should move swiftly to reverse the previous administration's withdrawal from the region and bring the United States back to the negotiating table.

[8] "Reps. Bera and Chabot Lead Bipartisan Members in Urging USTR to Pursue Digital Trade Agreement with Partners in Indo-Pacific," November 19, 2021

RESPONSES TO QUESTIONS SUBMITTED FOR THE RECORD

QUESTIONS FOR THE RECORD

APCAN Hearing

"Strategic Importance of Digital Economic Engagement in the Indo-Pacific"

Representative Dina Titus (NV-01)

---

1. Ms. Bliss, as you mentioned in your testimony, digital protectionism is on the rise throughout many countries in the region. These actions create barriers to digital trade, including censorship, filtering, localization measures, and regulations to protect privacy. The United States' message on digital protectionist policies has been somewhat inconsistent, this is due to the fact that many are not able to agree on what actually constitutes digital protectionism. How can the United States better lead in this space to ensure that barriers to digital trade, like censorship and filtering or restrictions to cross-border information, do not inhibit trade agreements with our allies and partners in the region?

QUESTIONS FOR THE RECORD

APCAN Hearing

"Strategic Importance of Digital Economic Engagement in the Indo-Pacific"

Representative Dina Titus (NV-01) to Ms. Wendy Cutler

Question: Ms. Cutler, in your written testimony you mention that you sense a degree of skepticism from counterparts in the region towards the proposed Indo-Pacific Economic Framework (IPEF), especially in contrast to China's move to join the CPTPP. In your view, how would our friends and competitors in the region respond to a new digital economy agreement that includes the most meaningful, inclusive, and forward-looking elements from existing agreements versus the digital components being developed in the IPEF?

Answer:

Ms. Cutler: Our allies and partners in the Indo-Pacific welcome strong U.S. economic engagement in the region. While they would prefer that the United States return to the CPTPP, they are also open to strengthening economic ties through the Indo-Pacific Economic Framework (IPEF) and have a great interest in robust engagement from the United States on the range of issues associated with the digital economy component. We understand that the digital economy will be one of the areas of focus of the IPEF, providing an important opportunity to include meaningful new commitments in this vital and emerging part of all of our economies.

Question: Ms. Cutler, ASEAN's digital economy is projected to grow to $1 trillion by 2030. ASEAN played a guiding role in negotiating the Regional Comprehensive Economic Partnership (RCEP) which contains its own digital rules and standards. How can the United States best engage ASEAN on digital issues in light of this and other digital economy agreements in the region, for instance those negotiated by Singapore?

Answer:

Ms. Cutler: In my view, the Indo-Pacific Economic Framework (IPEF) provides an important opportunity to strengthen ties with our ASEAN partners on a range of pressing regional economic matters, including those pertaining to the digital economy. But to effectively do so, it should be devised in a way that attracts the participation of Southeast Asian countries. One way to do so is to pursue a "modular" approach that is featured in the Digital Economy Partnership Agreement (DEPA), which in essence allows participants to agree to parts of the initiative at the outset, while signing on to others at a later stage when they are more prepared. Other means could include capacity building, private-public partnerships, and emphasis on boosting digital inclusiveness in the region, including strengthening digital tools available to SMEs.

QUESTIONS FOR THE RECORD

APCAN Hearing

"Strategic Importance of Digital Economic Engagement in the Indo-Pacific"

Representative Ann Wagner (MO-02) to Ms. Wendy Cutler

Question: With over 400 million internet users, ASEAN is quickly becoming a digital powerhouse. Ms. Cutler, what are ASEAN's priorities for a digital trade agreement? What are the key disagreements between the United States and ASEAN on digital policy issues, and how might we best overcome these differences?

Answer:

Ms. Cutler: As you well know as co-chair of the ASEAN Caucus, ASEAN is also composed of a diverse group of countries that are at differing levels of development and with differing approaches to digital policy. There is a strong interest, however, by governments across ASEAN on digital development and digital transformation. This includes areas such as education and digital skills, digital health, smart cities, connectivity, and cross-border data flows.

Beyond the IPEF, there are numerous avenues for strengthened U.S.-ASEAN cooperation on digital economy matters. I was pleased to see the U.S.-ASEAN Leaders' Statement on Digital Development as an outcome of the 9th ASEAN-U.S. Summit in October 2021. Last year, the U.S. met for the first time with the ASEAN Digital Ministers and continuing this high-level engagement is important. Some ongoing work which could be built upon includes cooperation through the ASEAN Digital Integration Index, the U.S.-ASEAN Connect Digital Economy Series and the Digital Connectivity and Cybersecurity Partnership (DCCP), as well as other initiatives on digital literacy and digital development. The Department of Commerce has also been supporting ASEAN's work on digital trade standards and I believe more can be done in this area. Finally, last year ASEAN agreed to begin negotiations on an internal ASEAN Digital Economy Framework Agreement. The U.S. should actively engage with ASEAN throughout this process, sharing best practices on what such an agreement could look like.

QUESTIONS FOR THE RECORD

APCAN Hearing

"Strategic Importance of Digital Economic Engagement in the Indo-Pacific"

Representative Ann Wagner (MO-02)

---

1. Mr. Feith, what provisions should a U.S.-led digital trade agreement include to slow or prevent the proliferation of PRC-style surveillance regimes, which authoritarian governments can use to establish invasive control over their own citizens?

ADDITIONAL INFORMATION MATERIALS SUBMITTED FOR THE RECORD

Written for the ITUC by: Duncan McCann, Senior Researcher, New Economics Foundation

New Economics Foundation
www.neweconomics.org
info@neweconomics.org
+44 (0)20 7820 6300
@NEF

Registered charity number 1055254

Cover: Adobe Stock

CONTENTS

FOREWORD

E-commerce proposals at the WTO: a recipe for corporate greed

Before the COVID-19 crisis, trust in governments and in democracy itself was collapsing around the world, 60 per cent of the world's workers were in informal jobs with no rights or protections and hundreds of millions of people who in employment were unable to make ends meet. The COVID-19 crisis is having catastrophic effects globally, compounding the existing weaknesses. The push for a WTO "e-commerce" agreement can only further exacerbate inequality and division at a time when the world needs to work as one. It is simply a recipe for yet more corporate greed. Governments are promoting new rules that would further reduce their own authority to regulate in the interests of people, to the extent that they are behaving more as captives of corporations, including giant tech monopolies, than as guardians of the public interest.

Digital technology holds enormous potential for tackling the world's most pressing problems on climate, poverty, inequality, health, education and much more. It has a massive role to play in tackling the spread of the SARS-CoV-2 virus and its consequences. It is now even more important that governments focus their efforts on harnessing technology for the common good, rather than simply being conduits for an agenda that would entrench corporate power and deepen inequality and mistrust.

This report, produced for the ITUC by the New Economics Foundation, reveals several deeply alarming impacts which would arise from an e-commerce agreement, while also exposing elements of some existing trade agreements which are of serious concern.

Control of data is at the heart of the proposals, and through that control of data, the power of digital behemoths such as Amazon would reach new heights. Their power is already far-reaching, due to the failure of governments to apply competition policy to prevent them dominating markets. This market dominance is set to grow even more if governments fail to ensure that the role tech companies play in the COVID-19 crisis in digital tracing and many other areas is done in the public interest with full respect for rights, instead of on the companies' terms.

The report highlights how an agreement on the lines proposed would increase precarious work leading to "Uberisation" of jobs, erode workers' rights, make regulation and enforcement more difficult and increase the power of Big Tech over workers.

With international concern over the implications of artificial intelligence and the deployment of algorithms without accountability, the planned provisions on secrecy of source code would allow corporations to maintain complete opacity and remove means by which victims of corporate malfeasance can achieve remedy for the damage done to them. The use of open source software in public procurement could also be challenged and negated.

It is important to note that the implications of such an e-commerce agreement would extend well beyond the tech sector itself. As data and digitalisation become central to business models in all sectors, rules concerning data affect every part of the economy and every worker, consumer and citizen.

The proposals would hamper, or in some cases eradicate, the potential for small and medium enterprises to grow and thrive, and would even reach into agriculture, where half of the world's workers work. Public services, already underfunded and under assault, would be further eroded by the incursion of digital monopolies into the provision of vital services, while the development of domestic industries, especially in countries which are not yet technologically advanced, would be impeded. Data protection regimes such as the EU's GDPR would also be undermined, and internet neutrality would be at risk.

Big Tech firms are seeking to use a WTO e-commerce agreement to tighten their grip on the global economy and squeeze yet more out of consumers and working people. Much of what they demand is not about trade at all; however, the WTO in its current form is a convenient back door to eliminate labour, privacy, property rights and other standards which are central to democracy.

Indeed, with almost half the world's population still locked out of the internet age, the mission to connect all the world's people must surely take precedence over a drive by some of the world's most powerful and least accountable corporations to extend their power and carve it into stone forever.

The international trade union movement will oppose the development of any agreement, at the WTO or elsewhere, which seeks to so fundamentally undermine the interests of working people and the public at large.

Sharan Burrow, General Secretary
International Trade Union Confederation

INTRODUCTION

When you navigate the internet, send messages or emails, and move around a city using map applications, you create data. These data, when properly analysed, can tell a lot about your behaviour. Big data companies gather your data in return of a "free" service – like an application that helps you measure calories – with your consent granted when you click "I agree" after a lengthy Terms of Use text that you never read.

The value of any one individual's data is pretty low on its own. However, when aggregated in millions of data points, trained algorithms can extract valuable conclusions about consumption, transportation, and work-related and other information. The conclusions are then used in order to target the right consumers at the right time and to pursue workplace rearrangements that would increase productivity.

Big data companies benefit hugely from this large information advantage, and are able to use it to transform the global economy and the world of work to suit their needs. These transformations are now happening outside of worker and democratic control. For instance, wearables, like smart watches, can tell software controllers how we work, and they use the data we produce in order to tighten worker surveillance and control, and potentially in some cases, automate us out of our jobs. Farming applications open up a world of previously unknown information about agricultural tasks, risks, inputs, and future yields that transform the nature of work in these sectors. Big data analytics enables companies to use this knowledge to increase their value-capture in supply chains and take over the value-adding while transforming the sector.

New technologies and the data revolution bear immense opportunities to answer humanity's challenges – global heating, poor quality work, hunger and diseases. However, history shows that not all technological revolutions reach everyone. About 1.2 billion people are still to get to the second industrial revolution when others are launching into the fourth one.

The technological revolution will not benefit us all automatically.

In fact, big companies and their host governments are already working hard to ensure that they maintain control over new technologies and that they set the rules of data governance. For this, they get their governments to agree to specific commitments in trade agreements. The first treaty to contain a whole e-commerce chapter was the 2003 Singapore-Australia free trade agreement (FTA).[1]

The 11th WTO Ministerial Conference may have ended without the adoption of a declaration, but a small number of initiatives were announced. One of them, which announced the intention to start negotiations on e-commerce, came from a group of 70 Members, mostly developed countries. The group was joined by six more countries, and in January 2019 the Members launched plurilateral e-commerce negotiations in the WTO, even though there is no WTO-wide mandate to do so, since a large group of developing countries managed to block the launch of official new negotiations on digital trade. The aim of the plurilateral negotiations is to agree to digital trade provisions that would ensure digital subordinance of small enterprises, a grave shift in the balance of bargaining power between capital and labour, and limited space for developing countries to digitalise with their own strategies.

The e-commerce agreement would create a framework that disciplines our governments' ability to regulate and enforce laws in cyberspace. Uber claims that they are a digital company, not a taxi company, and Fintech claims they provide e-services, not actual loans that should be governed by financial rules. Internet gives them the excuse to evade many aspects of national law and jurisdiction, including taxation. And they want that cemented.

The importance of e-commerce has grown with the development and expansion of the speed and reach of digital networks. In 2019, retail e-commerce sales worldwide amounted to $3.53 trillion and e-retail revenues are projected to grow to $6.54 trillion in 2022.[2] And just as digital is now permeating ever more sectors, the chapters in free trade agreements have also expanded to deal with many issues that are way beyond the original scope of facilitating trade over the internet.

1 Weber, R. (2015, September 10th). *The expansion of e-commerce in Asia-Pacific trade agreements*. Retrieved from https://www.ictsd.org/opinion/the-expansion-of-e-commerce-in-asia-pacific-trade-agreements
2 Statista (2019) *Retail e-commerce sales worldwide from 2014 to 2023*. Retrieved from https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/

For example, one of the most important new areas that is included in trade agreements is the demand for the free flow of data across borders. By including this in trade agreements, the aim is to help ensure that private ownership of data is the default and that transnational corporations should be able to freely move data around the world with minimal or no regulation.

The widening of the scope of the digital chapters along with data's centrality to global trade – it is estimated that in 2020 data flows account for more than 20 per cent of the world's GDP – has led to the WTO negotiations on "e-commerce", which is a deliberate misnomer for "data governance".

A common perception is that the EU and US are diametrically opposed on how their respective digital economies should function. But in fact the proposals from the two economic blocks are remarkably similar. There is one major and important exception, which is with regard to personal data privacy where the EU, through its implementation of the General Data Protection Regulation, has become the global proponent of privacy legislation.

A key element of the strategy has been to package together certain issues on which negotiators believe it will be possible to get agreement more easily, such as spam, authentication or recognising e-contracts, to act as a sort of Trojan horse in order to deliver the real intention of the chapters, which is to ensure the free flow of data across borders and eliminate data localisation requirements along with severely prohibiting source code disclosure

Although the digital revolution has been significant, it is important to remember that it is still a very recent innovation, with the internet recently celebrating its 30th birthday. This means that our institutions and policy framework are still adapting to the changes that the digital economy is driving in the way that we live, work and play.

This is even starker in developing countries, where four billion people do not have access to the internet. Developing countries are now putting in place the first efforts to develop a digital industrialisation agenda aiming at creating local economic activity. Many such countries are still in early stages for creating a legal framework for the protection of personal data and ensuring that digital innovation benefits working people.

Locking in global rules at such an early stage of the development of the internet and digital trade would lock in a status quo which sees ownership and control of data tightly concentrated in the hands of a few corporations while leaving states unable to maximise the public good that comes from digital innovation.

A COMPARATIVE ANALYSIS OF FREE TRADE AGREEMENT PROVISION

In this section we will explore four key texts – the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP), the US Mexico Canada Agreement (USMCA), the EU-Japan Economic Partnership Agreement, and the EU submission to the WTO (May 2019) – in order to complete a comparative legal analysis of the texts. The section will cover six different provisions in the digital trade chapter:

1. means of authentication and signatures and electronic contracts;
2. source code;
3. data flows;
4. data localisation;
5. data protection; and
6. open internet access.

In this section we make a number of overarching arguments with respect to the potential issues and impacts that arise from an analysis of the different provisions on digital trade. These are as follows:

- In general, the topics covered in the provisions are not specifically trade issues and therefore are inappropriate for inclusion in free trade agreements. The default position for policy on these topics, therefore, should be to regulate through domestic legislation wherever possible, especially where model legislation exists.
- Indeed, the inclusion of specific digital chapters in international trade agreements is designed to limit the ability of domestic governments to regulate in key emerging areas of the digital economy.
- Digital technologies are already impacting and disrupting our economy irrespective of how and whether they are included in international trade agreements. Nonetheless, these digital chapters will in many instances exacerbate the existing risks of adverse social and economic effects arising from digital disruption by locking in a liberal, under-regulated environment.
- As data and algorithms become ever more central components of our social and economic lives, the importance of digital trade provisions in international trade agreements will also grow.

MEANS OF AUTHENTICATION AND E-SIGNATURES AND ELECTRONIC CONTRACTS

CPTTP	EU-Jap	USMCA	EU Submission to WTO
Article 14.6: Electronic Authentication and Electronic Signatures	Article 8.77 Electronic authentication and electronic signature	Article 19.6: Electronic Authentication and Electronic Signatures	2.2 ELECTRONIC AUTHENTICATION AND ELECTRONIC SIGNATURES
1. Except in circumstances otherwise provided for under its law, a Party shall not deny the legal validity of a signature solely on the basis that the signature is in electronic form.	Unless otherwise provided for in its laws and regulations, a Party shall not deny the legal validity of a signature solely on the grounds that the signature is in electronic form.	1. Except in circumstances provided for under its law, a Party shall not deny the legal validity of a signature solely on the basis that the signature is in electronic form.	1. Members shall not deny legal effect and admissibility as evidence in legal proceedings of electronic signature solely on the basis that it is in electronic form.
2. No Party shall adopt or maintain measures for electronic authentication that would: (a) prohibit parties to an electronic transaction from mutually determining the appropriate authentication methods for that transaction; or (b) prevent parties to an electronic transaction from having the opportunity to establish before judicial or administrative authorities that their transaction complies with any legal requirements with respect to authentication.	2. A Party shall not adopt or maintain measures regulating electronic authentication and electronic signature that would: (a) prohibit parties to an electronic transaction from mutually determining the appropriate electronic authentication methods for their transaction; or (b) prevent parties to electronic transactions from having the opportunity to establish before judicial or administrative authorities that their electronic transactions comply with any legal requirements with respect to electronic authentication and electronic signature.	2. No Party shall adopt or maintain measures for electronic authentication and electronic signatures that would: (a) prohibit parties to an electronic transaction from mutually determining the appropriate authentication methods or electronic signatures for that transaction; or (b) prevent parties to an electronic transaction from having the opportunity to establish before judicial or administrative authorities that their transaction complies with any legal requirements with respect to authentication or electronic signatures.	2. Members shall ensure that parties to an electronic transaction are not prevented from: (a) mutually determining the appropriate electronic authentication methods for their transaction; (b) being able to prove to judicial and administrative authorities that the use of electronic authentication or an electronic signature in that transaction complies with the applicable legal requirements.
3. Notwithstanding paragraph 2, a Party may require that, for a particular category of transactions, the method of authentication meets certain performance standards or is certified by an authority accredited in accordance with its law.	3. Notwithstanding paragraph 2, each Party may require that, for a particular category of transactions, the method of authentication meets certain performance standards or is certified by an authority accredited in accordance with its laws and regulations.	3. Notwithstanding paragraph 2, a Party may require that, for a particular category of transactions, the electronic signature or method of authentication meets certain performance standards or is certified by an authority accredited in accordance with its law.	3. Notwithstanding paragraph 2, certification requirements by an authority accredited in accordance with domestic law or certain performance standards may apply for a particular category of transactions, the method of authentication or electronic signature. Such requirements and standards shall be objective, transparent and non-discriminatory and shall only relate to the specific characteristics of the category of transactions concerned.
4. The Parties shall encourage the use of interoperable electronic authentication.		4. Each Party shall encourage the use of interoperable electronic authentication.	4. To the extent provided for under domestic law, Members shall apply paragraphs 1 to 3 to other electronic processes or means of facilitating or enabling electronic transactions, such as electronic time stamps, electronic registered delivery services or website authentication.

When people and companies trade, there need to be ways to validate both the details of the transaction and that the people and companies engaging in the transaction are who they claim to be. Technology that enables electronic authentication and e-signature are vital to this process. The battle in this area is between businesses that want the minimum number of laws and regulations specifying, limiting or restricting the use of electronic authentication, versus the public interest, i.e., ensuring that the domestic digital trade environment is safe and secure.

This provision is specifically being pushed by the EU, which has had an e-signature directive since 1999, recently updated by the Electronic Identification and Trust Services for Electronic Transactions Regulation (better known as the eIDAS Regulation) which came into force in July 2016. Due to these earlier regulations and the efforts of EU businesses to comply, this is an area where the EU has a leadership position from a technology perspective, and so there is a direct opportunity to drive business by putting these requirements in treaties.

Although overall provisions on electronic authentication and e-signature appear in only half of trade agreements[3], they appear in detailed form in all four of the documents that we looked at in detail.

This is a section where the marked similarity in the texts is what stands out. The key point that they all reinforce is that "A party shall not deny the legal validity of a signature solely on the basis that the signature is in electronic form." This should be read together with the text that prohibits governments from adopting or maintaining any requirements which would "prohibit parties to an electronic transaction from mutually determining the appropriate authentication methods for that transaction" and, if challenged, that those parties should be able to argue in court as to the validity of the signature. The key point that they want to reinforce is that it should not be up to the government to tell two (or more) parties that are engaged in a transaction what technology, system or implementation model they should use. Instead, the free trade agreements stipulate that it should be up to the parties to the transaction itself to determine what the best authentication technology to use is.

The CPTPP and USMCA and the EU-Japan text all start with the same exemption that the provisions apply "Except in circumstances otherwise provided for under its law." It is interesting that the EU submission to the WTO does not contain the same phrase, since it would seem to be an important derogation that clearly has wide support among other countries, including the EU itself, since it forms part of the EU-Japan text. Finally, they all allow governments to establish performance standards "for a particular category of transactions", without in any way defining what those categories could be. The phrasing of these powers together with the fact that they do not have to secure a legitimate public policy objective could mean that these will provide governments enough room to ensure that transactions that require high levels of security, such as finance or identity, could be legislated for. Again, the CPTPP and USMCA and the EU-Japan text specifically allow for the ability of governments to require that authentication protocols are "certified by an authority accredited in accordance with its law". The EU submission on the other hand provides considerable detail on the limits of the actions of government in this regard. It seeks to require that all requirements are "objective, transparent and non-discriminatory and shall only relate to the specific characteristics of the category of transactions concerned."

Part of the challenge of deciphering the actual impacts of these various provisions is that two key terms remain undefined, namely "parties" and "electronic transaction". So although the parties to the agreements may know how they apply, it is very hard for those without the definitions to come to firm judgements.

What we can do is highlight some potential problems with allowing parties to decide between themselves which authentication technology to use.

- Firstly, there is an efficiency agreement which holds that in a world of multiple private authentication standards, there is additional cost due to lack of interoperability and the need to manage multiple systems.
- Secondly, dominant companies could set standards, which often are expensive to comply with, and then penalise those who do not comply. A recent example involved Visa and Mastercard and their implementation of anti-fraud software in their merchant network with the stated purpose of ensuring that the payment system was secure. However, the scheme has been called a "near scam" by the National Retail Federation in the US, and in a legal challenge it was asserted that "the system is less a system for securing customer card data than a system for raking in profits for the card companies via fines and penalties."[4]
- Thirdly, there is also the serious risk that the standard being pushed by companies is not secure enough. As Richard Hill notes, governments often have to intervene due

3 Wu, M. (2017). *Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for Multilateral Trade System*. RTA Exchange. Retrieved from http://e15initiative.org/wp-content/uploads/2015/09/RTA-Exchange-Digital-Trade-Mark-Wu-Final-2.pdf

4 Zetter, K. (2012, November 1). *Rare legal fight takes on credit card company security standard and fines*. Retrieved from https://www.wired.com/2012/01/pci-lawsuit/

to market failure because "externalities associated with insufficient security: the costs of a security breach are borne largely by entities other than the company that suffered the breach because of inadequate security."[5]

- Finally, there are also good consumer protection grounds for government setting standards, since otherwise consumers may struggle to understand whether the myriad of authentication technologies are really secure.

Ultimately, this topic is not well suited to being set down in free trade agreements. The model law[6] proposed by UNCITRAL is a much better way to incorporate these requirements into national law frameworks because it allows countries the opportunity to adapt the legislation to local needs and requirements.

5 Hill, R. (2017). *Notes on & E-signatures and Trade*. Our World is Not for Sale. Retrieved from https://ourworldisnotforsale.net/2017/Hill_E-signatures.pdf
6 UNCITRAL (2001) *Model law on electronic signatures with guide to enactment*. Retrieved from https://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf

SOURCE CODE

CPTTP	EU-Japan	USMCA	EU Submission to WTO
Article 14.17: Source Code 1. No Party shall require the transfer of, or access to, source code of software owned by a person of another Party, as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory. 2. For the purposes of this Article, software subject to paragraph 1 is limited to mass-market software or products containing such software and does not include software used for critical infrastructure. 3. Nothing in this Article shall preclude: (a) the inclusion or implementation of terms and conditions related to the provision of source code in commercially negotiated contracts; or (b) a Party from requiring the modification of source code of software necessary for that software to comply with laws or regulations which are not inconsistent with this Agreement. 4. This Article shall not be construed to affect requirements that relate to patent applications or granted patents, including any orders made by a judicial authority in relation to patent disputes, subject to safeguards against unauthorised disclosure under the law or practice of a Party.	Article 8.73: Source Code 1. A Party may not require the transfer of, or access to, source code of software owned by a person of the other Party. Nothing in this paragraph shall prevent the inclusion or implementation of terms and conditions related to the transfer of or granting of access to source code in commercially negotiated contracts, or the voluntary transfer of or granting of access to source code, for instance in the context of government procurement. 2. Nothing in this Article shall affect: (a) requirements by a court, administrative tribunal or competition authority to remedy a violation of competition law; (b) requirements by a court, administrative tribunal or administrative authority with respect to the protection and enforcement of intellectual property rights to the extent that source codes are protected by those rights; and (c) the right of a Party to take measures in accordance with Article III of the GPA. 3. For greater certainty, nothing in this Article shall prevent a Party from adopting or maintaining measures which are inconsistent with paragraph 1, in accordance with Articles 1.5, 8.3 and 8.65.	Article 19.16: Source Code 1. No Party shall require the transfer of, or access to, a source code of software owned by a person of another Party, or to an algorithm expressed in that source code, as a condition for the import, distribution, sale or use of that software, or of products containing that software, in its territory. 2. This Article does not preclude a regulatory body or judicial authority of a Party from requiring a person of another Party to preserve and make available the source code of software, or an algorithm expressed in that source code, to the regulatory body for a specific investigation, inspection, examination, enforcement action, or judicial proceeding, subject to safeguards against unauthorized disclosure	2.6 Transfer or access to source code 1. Members shall not require the transfer of, or access to, the source code of software owned by a natural or juridical person of other Members. 2. For greater certainty: (a) the general exception, the security exception as well as the exceptions in the paragraph 2 of the GATS Annex on Financial Services apply to measures adopted or maintained in the context of a certification procedure; (b) paragraph 1 does not apply to the voluntary transfer of or granting of access to source code on a commercial basis by a natural or juridical person, for instance in the context of a public procurement transaction or a freely negotiated contract. 3. Paragraph 1 is without prejudice to: (a) requirements by a court, administrative tribunal, or by a competition authority to remedy a violation of competition law; (b) the protection and enforcement of intellectual property rights; and (c) the right to take any action or not disclose any information that is considered necessary for the protection of essential security interests relating to the procurement of arms, ammunition or war materials, or to procurement indispensable for national security or for national defence purposes.

Source code is the set of instructions or rules that a computer programme follows, and is written in a way that humans can understand. It is used for everything from software in our phones, smart appliances and cars, to the algorithms used to sort information for us on the internet, such as Google's search engines or Facebook's newsfeed, to the protocols that manage our traffic lights and national energy infrastructure.

Source code is already included in intellectual property and trade secrets protections across the globe. Where subject to patent protection, it is already an offence for a person, company or government to access, share or copy source code, without legal justification. Patent protection often requires the party seeking protection to divulge the code to the patent office. For those not wishing to do that, they could still use trade secrets protection to ensure their code is not improperly accessed or shared. Trade secrets are protected by Article 39 of the WTO's Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). This provision in the digital

trade chapter is therefore concerned solely with the power of governments and their agents, like courts and regulators, to take actions that would require the transfer of or access to source code as a condition of being allowed to operate in a particular country.

It is important to stress that there are many legitimate reasons why a government may require a company to share their source code. Contemporary examples of governments range from requiring it for specific legal cases, such as intellectual property disputes, to more general reasons, like ensuring economic stability or investigating potential biases. Here are some examples of governments legally requesting source code that may not be permitted under currently agreed and proposed free trade agreements:[7]

- Some financial regulators, such as the US, require firms operating High Frequency Trading algorithms to disclose their source code so that the regulators can "review code, training data and proprietary formulas" to understand what had caused previous flash crashes[8] in the stock market and to prevent them happening in the future.[9]
- A significant proportion of gambling is now done through electronic machines, apps and websites where the odds of winning is determined by software. The gambling regulators therefore check the source code running electronic gambling machines to ensure that the chance of winning is fairly programmed.[10]
- Toyota cars were involved in a number of suspicious accidents resulting in death. They were required to hand over their source code to regulators who engaged NASA to analyse the data. Although they were not able to find a smoking gun, they found enough to force the company to hand it over to the victim's IT consultants, who found the root of the problem.[11]

Helping to bridge the digital divide through technology transfer has been a legitimate expectation in some sectors for some countries,[12] although seen as a trade barrier in the US.[13] As more and more products and services are run by source code, the prohibition on the requirement to share it as a condition of market access would make technology transfer involving source code illegal under the trade agreement.

Although there is considerable divergence between the four treaty texts analysed, there is overwhelming agreement on the core of what the section should cover, namely that "No Party shall require the transfer of, or access to, source code of software owned by a person of another Party." Only the USMCA adds to this by extending what is covered to include "an algorithm expressed in that source code". The CPTPP and USMCA also stipulate explicitly what the other texts appear to assume, namely that the source code cannot be required to be shared or accessed "as a condition for the import, distribution, sale or use of that software, or of products containing that software, in its territory".

The extension of the exclusion to algorithms in the USMCA poses a new and more serious challenge even when compared with the already problematic source code provisions. An algorithm is different from the source code itself in so far as it describes the basic logic that a computer program should follow. An algorithm can be understood as a recipe that involves a series of sequential steps with options and decision points, whereas source code is the language and form by which these instructions are written by people to be interpreted by computers. But at the core of an algorithm is ultimately an idea, and as such not currently specifically protected under existing intellectual property regimes. TRIPS has already allowed companies to start to use trade secrets protection for their algorithms. The US proposal goes far beyond this and extends the already problematic protections for source code to the algorithms themselves.

The bulk of the sections on source code are concerned with the instances when the agreed prohibition on sharing source code can be overridden. The evolution of the exceptions is a perfect example of the challenges of agreeing text on matters which continue to evolve rapidly and where some may fail to foresee the full implications of what they are signing up to. The Japan-Mongolia agreement, the first to contain such a provision, only had an exception for critical infrastructure. In the CPTPP the parties realised that carving such a narrow exception list

7 Smith, SR. (2017, December 10) *Some preliminary implications of WTO source code proposal.* Third World Network Briefings. Retrieved from https://www.twn.my/MC11/briefings/BP4.pdf

8 A flash crash is an event in electronic securities markets wherein the withdrawal of stock orders rapidly amplifies price declines. The result appears to be a rapid sell-off of securities that can happen over a few minutes, resulting in dramatic declines.

9 Rieke, A. Bogen, M. & Robinson, D. (2018) *Public Scrutiny of Automated Decisions: Early lessons and Emerging Methods.* Upturn and Omidyar Network. Retrieved from https://www.omidyar.com/sites/default/files/file_archive/Public%20Scrutiny%20of%20Automated%20Decisions.pdf

10 Gambling Commission (2018). *Testing strategy for compliance with remote gambling and software technical standards.* Retrieved from http://www.gamblingcommission.gov.uk/pdf/Testing-strategy-for-compliance-with-remote-gambling-and-software-technical-standards.pdf

11 Safety Research & Strategies Inc. (2013, November 7) *Toyota Unintended Acceleration and the big bowl of Spaghetti code.* Retrieved from http://www.safetyresearch.net/blog/articles/toyota-unintended-acceleration-and-big-bowl-%E2%80%9Cspaghetti%E2%80%9D-code

12 Smith, SR. (2017, December 10) *Some preliminary implications of WTO source code proposal.* Third World Network Briefings. Retrieved from https://www.twn.my/MC11/briefings/BP4.pdf p.4

13 Fefer, R. (2019 March 29) *Digital Trade.* Congressional Research Service. Retrieved from https://fas.org/sgp/crs/misc/IF10770.pdf

would undermine the way that patent law generally works, which requires the handing over of the code in order to get the protected monopoly status.

They therefore expanded the exceptions to include patent law. TiSA extended the exception to legitimate public policy objective (including competition law), albeit knowing that Parties have historically found it very difficult to satisfy the exemption, due to the narrow way in which the legitimate public policy test has been interpreted in the case law.[14] In the EU's submission to the WTO they have listed the exemptions more specifically to include competition law, intellectual property and national security considerations. Finally, the USMCA decided to try another route altogether by no longer trying to create an exhaustive list of fields in which access to source code could be required but instead chose to focus on setting out who could legitimately request the data under which circumstances. In the formulation of the USMCA, as long as the requirement to share source code comes from a "regulatory body or judicial authority" for the purpose of an "investigation, inspection, examination, enforcement action, or judicial proceedings", then it should be permitted. The addition of the word "specific" can be seen as protection against blanket requirements by parties, meaning the source code could only be accessed in specific cases once some form of official proceedings had been instigated by the state.

Another serious issue identified in the EU–Japan FTA and the EU submission to the WTO is that although it allows governments to require disclosure of source codes to remedy a violation of competition laws, it is debatable whether the language would cover the disclosure of the code in order to prove whether a violation had taken place. Yet this is an almost essential prerequisite to the need for a remedy itself. A recent example can be seen from the automotive industry, where Volkswagen's fraudulent software for monitoring emissions was only confirmed when non-state researchers were able to analyse the source code – something that may not be possible in the future.

The evolution of exemptions within the agreements is normal and demonstrates the problem with locking in specific detailed rules before we really understand what is required and the full range of exemptions needed. Although it is clear that in the more recently ratified agreements and proposals, such as the USMCA or the EU submission to the WTO, the exemptions are better drafted, they still leave important cases where source code should be shared unexpressed. As the examples cited earlier show, the non-disclosure of source code poses problems beyond the narrow realms of competition, intellectual property and national security. The USMCA acknowledges this, but its focus on disclosure "to the regulatory body" means that in important cases it may not be possible to share the source code with specialist lawyers or technology experts who are often key to establishing whether there is a case to answer and any remedy may be required. Allowing non-disclosure to these kinds of actors to become the norm will make it much harder to monitor the performance and ensure the compliance of corporate source code. Even getting the text perfect still poses problems for agreements that have already been signed, since the texts do not update automatically as problems are identified and drafting improved.

The proposal around source code supports the corporate strategy that businesses should endeavour to keep their code secret in order to maximise their profit. However, this may not be the best way to keep us all secure. The US Department of Defense prefers to work with open source software because "making source code available to the public significantly aid[s] defenders ... and improves reliability and security." This reasoning shows why we should be very cautious about accepting the notion that source code, and the algorithms that they run, are best kept secret – especially as the areas that will be governed by such code are ever expanding through digitisation and automation. Ultimately, as the Open Rights Group have noted, "these clauses could be used to challenge any public procurement perceived to give preference to open source."[15]

The extension of the prohibition to request source code beyond that already enshrined in patent and trade secret protection represents a brazen attack on the ability of government to ensure that software, in its myriad of applications, is keeping us and our data safe, secure and private.[16] And it is also a short-sighted attack, in terms of the longer-term interests of Western geo-political interests. This is because just as the provision prevents a country demanding to see proprietary code from one of the US tech giants, as was the drafters' principal intention, it will also prevent US and EU governments from looking into Chinese or Russian code as well.

14 World Trade Organisation. *Technical Information on Technical Barriers to Trade*. Retrieved from https://www.wto.org/english/tratop_e/tbt_e/tbt_info_e.htm
15 Ruiz, J. (2019, March 14) *US red lines for digital trade with the UK cause alarm*. Retrieved from https://www.openrightsgroup.org/blog/2019/us-red-lines-for-digital-trade-with-the-uk-cause-alarm
16 Knowledge Ecology International. (2015, December 29) *KEI statement on TPP for the January 12, 2016 hearing of the United States International Trade Commission*. Retrieved from https://www.keionline.org/wp-content/uploads/KEI-USITC-TPP-29Dec2015.pdf

CROSS-BORDER DATA FLOWS

CPTTP	EU-Jap	USMCA	EU Submission to WTO
Article 14.13: Location of Computing Facilities 1. The Parties recognise that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications. 2. No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory. 3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.	Article 8.81 Free Fow of Data The Parties shall reassess within three years of the date of entry into force of this Agreement the need for inclusion of provisions on the free flow of data into this Agreement.	Article 19.12: Location of Computing Facilities No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.	2.7 CROSS-BORDER DATA FLOWS 1. Members are committed to ensuring cross-border data flows to facilitate trade in the digital economy. To that end, cross-border data flows shall not be restricted by: (a) requiring the use of computing facilities or network elements in the Member's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of the Member; (b) requiring the localization of data in the Member's territory for storage or processing; (c) prohibiting storage or processing in the territory of other Members; (d) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Member's territory or upon localization requirements in the Member's territory.

As the digital economy grows and sectors increasingly rely on data as a key input to almost any business they need, especially for large multinational businesses, to move data easily across national borders is becoming a key demand of industry.[17] The aggregation of massive datasets from multiple countries holds out the possibility of helping address some of our global challenges as well as boost global trade and improve our health. A senior employee at the OECD underlined the importance of cross-border data flows for the wider trade negotiations when he stated that "data flows are important, you just won't believe how mind-bogglingly important they are for trade today."[18] While this can be the case, and where possible, data flows should be enabled, this is not the same as demanding that all forms of data, especially that which is personal and sensitive, should be able to cross the border freely without any restriction, control or oversight.

A very interesting aspect to the provisions around cross-border data flows is that there are no common clauses that are shared across all the four key texts that are under analysis reflecting the fact that there is considerable disagreement between key parties. There is commonality in the case of the two US-related texts and again in the case of the two EU-related texts. This reflects the different way that the US and the EU view the cross-border data flows.

In the EU-Japan agreement, there is no provision around free flow of data – only a commitment to look at the issue again in three years time.

Both the CPTPP and USMCA seek to make the free flow of data the default position with both of them requiring parties to "allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person." One interesting point is that the CPTPP frames the obligation in the positive

17 The Software Alliance (2017) *Cross-Border Data Flows*. Retrieved from https://www.bsa.org/files/policy-filings/BSA_2017CrossBorderDataFlows.pdf
18 Gonzalez, JL. (2019, June 3) Don't panic! The hitcheker's guide to cross-border data flows. OECD. Retrieved from https://www.oecd.org/trade/hitchhikers-guide-cross-border-data-flows/

that "each party shall allow" whereas the USMCA states that "no party shall prohibit". Although both the CPTPP and the USMCA allow parties to adopt measures to constrain the free flow of data when this "achieves a legitimate public policy objective", this has rarely enabled countries the policy freedom that a layman's reading of the words suggests. This is because "legitimate" has been interpreted in a WTO dispute to mean widely recognised policy solution,[19] while only considering protecting health, environment and privacy as acceptable. This means that novel approaches in sectors, especially ones undergoing digital transformation, could be ruled illegitimate, even when concerned with health, environment or privacy, despite being a valid policy objective. This is especially true when combined with the necessity test that a policy does not "impose restrictions on transfers of information greater than are required to achieve the objective." This has meant that in 44 attempts to use this method to derogate from a particular provision, only one has been successful.

Probably most interestingly, the EU submission to the WTO has a much weaker commitment to cross-border flows when it states that "Members are committed to ensuring cross-border data flows to facilitate trade in the digital economy." The requirement to "commit to ensure" cross-border flows offers parties much greater freedom to restrict cross-border flows than the USMCA's text, which states: "No Party shall prohibit or restrict the cross-border transfer." Because the EU wording offers greater flexibility to the parties, there is no need to balance a strong prohibition with a series of complex derogations.

What is interesting is that the EU clearly considers this compatible with the General Data Protection Regulation (GDPR), which is the most stringent data protection regime in the world, even when far from perfect. Indeed, Wilbur Ross, US Commerce Secretary, has openly called GDPR an unnecessary barrier to trade.[20]

Under GDPR, companies and the public sector operating in the EU, as well as those handling the data of EU citizens outside the EU, must take measures to protect personal data, something that would almost certainly contravene the provisions in the CPTPP and USMCA, since it would represent a restriction, at the very least, on the cross-border transfer of information, even if that information were personal and too sensitive. This means that the EU will never be able to sign up to such a provision as worded in the USMCA or CPTPP.

It will be interesting to see how the UK proceeds in negotiating its new trade deals given the pressure it will be under to accept US terms to ensure a quick trade deal can be signed while at the same time still having the EU's GDPR on the statute books.

19 World Trade Organisation. *Canada – Patent Protection of Pharmaceutical Products*. Retrieved from http://www.wto.org/english/tratop_e/dispu_e/cases_e/ds114_e.html
20 Ross, W. (2018 May 18) *EU data privacy laws are likely to create barriers to trade*. Retrieved from https://www.ft.com/content/9d261f44-6255-11e8-bdd1-cc0534df682c

DATA LOCALISATION

CPTTP	EU-Japan	USMCA	EU Submission to WTO
Article 14.13: Location of Computing Facilities 1. The Parties recognise that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications. 2. No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory. 3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.		Article 19.12: Location of Computing Facilities No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.	2.7 Cross-Border Data Flows 1. Members are committed to ensuring cross-border data flows to facilitate trade in the digital economy. To that end, cross-border data flows shall not be restricted by: (a) requiring the use of computing facilities or network elements in the Member's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of the Member; (b) requiring the localization of data in the Member's territory for storage or processing; (c) prohibiting storage or processing in the territory of other Members; (d) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Member's territory or upon localization requirements in the Member's territory.

Data localisation requirements – where companies are obligated to locate some or all of their equipment that collects, analyses and transfers data internationally within a particular country – have become the topic of important geopolitical debate. At one extreme of the debate, there is Russia, where all personal data collected from all Russians must be stored and processed domestically.[21] Other countries take a more targeted approach focusing only on certain strategically important or particularly sensitive categories of data, such as Nigeria, which requires government data to be stored within the country, and Australia, which only allows health data out of the country (effectively mandating local storage) in a very narrow set of circumstances. At the other extreme, global tech companies want to see a ban on localisation requirements, viewing them as an impediment that will "limit access to global services" because of the additional cost it imposes on the companies and is seen by the global free trade community as "the principal instrument for protectionism in the information age".[22]

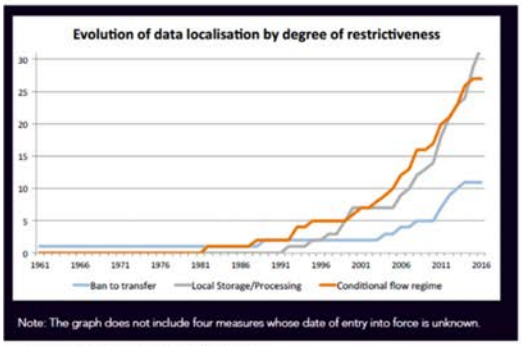
Although localisation requirements have been increasing since the 1990s, as the graph below shows, the TPP, predecessor of the CPTPP, was the first trade agreement to contain such a specific provision severely limiting the contexts in which any form of data localisation is permitted.

There are no common provisions across the four treaties due to the EU-Japan deal failing to include a specific clause on the subject. However, the CPTPP, USMCA and EU submission to the WTO all agree it should never be permissible for countries to require data localisation as a prerequisite for gaining market access to that country. They make this very clear when they state that "no Party shall require a

21 Bowman, C (2017, January 6) *Data Localization Laws: an emerging global trend*. Retrieved from http://jurist.org/hotline/2017/01/data-localization-laws-an-emerging-global-trend.php

22 Chander, A. (2018, October 9) *The coming north American digital trade zone*. Council on Foreign Relations. Retrieved from https://www.cfr.org/blog/coming-north-american-digital-trade-zone

covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory."



Source: ECIPE, Digital Trade Estimates Database

However, the three texts differ greatly when it comes to articulating the circumstances under which parties may apply data localisation requirements, technically known as derogations. The USMCA in effect bars all data localisation requirements in all cases – even for financial (it does so under a different set of rules set forth in the financial services chapter) or health data, two cases where there is a strong justification for requiring it to be stored locally.

The CPTPP does contain a derogation that at first reading seems to allow parties quite a wide margin to operate in. The text states this in relation to data localisation requirements that pursue a "legitimate public policy objective", which includes health, the environment and privacy. However, this wide ranging set of objectives is qualified and constrained by the requirement that it is no greater than the required. This has generally been interpreted quite narrowly within the case law, and the practical experience of attempting to use the derogation tells us that it does not provide the policy space the some countries want in this important area.

There are good arguments both for and against imposing data localisation requirements. As well as the arguments put forward by Big Tech, some digital rights groups also work to limit data localisation requirements. Digital rights groups fear that localisation requirements can be used to "facilitate restrictions on freedom of expression by national governments"[23] as they force tech companies to store data locally which they can then access easily, unlike data stored in a third country. In addition, businesses based in some countries are against data localisation because the local digital infrastructure is of poor quality.[24]

However, arguments for data localisation are also strong. Many are concerned by the amount of data held about us by the tech giants and that localisation could help the development of a more decentralised data infrastructure. This becomes especially important in the context of a growing appetite of countries to develop their own national AI capabilities, since data is the key resource for increasing the capabilities of AI-related technology. There are also a myriad of public policy objectives which could legitimately require data localisation such as a regulatory oversight of the financial system, or other sectors, and national security objectives.

We do not seek to come to a final decision on whether data localisation is good or bad but instead highlight the complexity of the ongoing debate in the subject. One aspect that is very hard to reconcile concerns factors like localisation (which may cause global tech companies to withdraw from the country, leading to impacts for local people and businesses who are not able to use their services) balanced against the fact that the absence of the tech giants may be the only way to ensure that domestic alternatives emerge, since they can be almost impossible to develop in an open and free market. Indeed, our main conclusion in this section is that this area is not suitable to be part of trade negotiations. India is playing a high profile role in this regard and wishing to retain the right to implement data localisation requirements was one of the reasons for its recent rejection of the e-commerce chapter of the Regional Comprehensive Economic Partnership (RCEP) agreement.[25]

23 Ruiz, J. (2018, November 23) *Open Rights Group submission to UK consultation on a new free trade agreement with the United States of America*. Retrieved from https://www.openrightsgroup.org/assets/files/pdfs/submissions/org_fta_consultation_usa.pdf
24 Chander, A. & Uyen, P. (2015 March 13). *Data Nationalism*. Emory Law Journal, Vol. 64, No. 3, 2015. Available at SSRN: https://ssrn.com/abstract=2577947
25 Raghavan, T.C.A. (2019, October 11) *India rejects RCEP e-commerce chapter*. The Hindu. Retrieved from https://www.thehindu.com/business/India-rejects-rcep-e-commerce-chapter/article29659912.ece

DATA PROTECTION

CPTTP	EU-Japan	USMCA	EU Submission to WTO
Article 14.8: Personal Information Protection5 1. The Parties recognise the economic and social benefits of protecting the personal information of users of electronic commerce and the contribution that this makes to enhancing consumer confidence in electronic commerce. 2. To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce. In the development of its legal framework for the protection of personal information, each Party should take into account principles and guidelines of relevant international bodies. 3. Each Party shall endeavour to adopt non-discriminatory practices in protecting users of electronic commerce from personal information protection violations occurring within its jurisdiction. 4. Each Party should publish information on the personal information protections it provides to users of electronic commerce, including how: (a) individuals can pursue remedies; and (b) business can comply with any legal requirements. 5. Recognising that the Parties may take different legal approaches to protecting personal information, each Party should encourage the development of mechanisms to promote compatibility between these different regimes. These mechanisms may include the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement, or broader international frameworks. To this end, the Parties shall endeavour to exchange information on any such mechanisms applied in their jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility between them.	Article 8.78 Consumer protection 3. The Parties recognise the importance of adopting or maintaining measures, in accordance with their respective laws and regulations, to protect the personal data of electronic commerce users.	Article 19.8: Personal Information Protection 1. The Parties recognize the economic and social benefits of protecting the personal information of users of digital trade and the contribution that this makes to enhancing consumer confidence in digital trade. 2. To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade. In the development of this legal framework, each Party should take into account principles and guidelines of relevant international bodies, such as the APEC Privacy Framework and the OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013). 3. The Parties recognize that pursuant to paragraph 2, key principles include: limitation on collection; choice; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and accountability. The Parties also recognize the importance of ensuring compliance with measures to protect personal information and ensuring that any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented. 4. Each Party shall endeavor to adopt non-discriminatory practices in protecting users of digital trade from personal information protection violations occurring within its jurisdiction. 5. Each Party shall publish information on the personal information protections it provides to users of digital trade, including how: (a) a natural person can pursue a remedy; and (b) an enterprise can comply with legal requirements. 6. Recognizing that the Parties may take different legal approaches to protecting personal information, each Party should encourage the development of mechanisms to promote compatibility between these different regimes. The Parties shall endeavor to exchange information on the mechanisms applied in their jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility between them. The Parties recognize that the APEC Cross-Border Privacy Rules system is a valid mechanism to facilitate cross-border information transfers while protecting personal information.	2.8 Protection of Personal Data and Privacy 1. Members recognize that the protection of personal data and privacy is a fundamental right and that high standards in this regard contribute to trust in the digital economy and to the development of trade. 2. Members may adopt and maintain the safeguards they deem appropriate to ensure the protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data. Nothing in the agreed disciplines and commitments shall affect the protection of personal data and privacy afforded by the Members' respective safeguards. 3. Personal data means any information relating to an identified or identifiable natural person.

The amount of data we create and share as part of our normal daily lives is increasing exponentially. Ninety per cent of the world's data was created in the last two years, and over 2.5 billion gigabytes of data are produced every day, equivalent to filling over 19.5 million new iPads.[26] Whole companies are built around the principle of relentlessly collecting as much data about internet users as possible, in order to monetise it. The EU has taken the lead in implementing legislation, the General Data Protection Regulation, which requires companies to seek consent when collecting data and governs how they can use and share or sell this data to third parties. This is at odds with most of the rest of the world, exemplified by the US, which has only the most minimal protections for data in place.

This means that the provisions on data protection are without doubt some of the most controversial and difficult, since the fundamental positions of the main

26 Assuming maximum standard iPad storage of 128GB (https://www.apple.com/uk/ipad-10.2/)

negotiating parties (US and EU[27]) are so diametrically opposed.

The texts pertaining to data protections across the four treaties start in reasonably similar fashion – although the small differences actually tell us a lot of the positions of the negotiating parties. In the CPTPP, EU-Japan agreement and USMCA, they all commit to "recognize the economic and social benefits of protecting the personal information." The EU submission to the WTO, however, takes this further by recognising that "the protection of personal data and privacy is a fundamental right." This difference in language between the two is significant, since one merely recognises that there could be a social and economic benefit from implementing data protection policies and leaves countries able to implement legislation, whereas the EU submission phrases "data protection" and "fundamental right" in such a way that arguably requires states to act. This exposes the fundamentally different way that the EU and US view the protection of people's data. The language in the EU-Japan agreement is a mix between the US lead texts of USMCA and CPTPP and the EU submission to WTO by framing data protection legislation as valid and acknowledging existing laws without going as far as calling it a "fundamental right".

The CPTPP and USMCA both seem to require the state to take some positive action to "adopt or maintain a legal framework that provides for the protection of the personal information." However, the clause has an important footnote which provides that "a Party may comply with the obligation in this paragraph by ... laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy." This would allow a party to comply merely by placing some oversight on existing voluntary data protection regimes. Voluntary corporate compliance regimes have failed to achieve the aims for which they were implemented[28],[29] and given some of the challenges in enforcing the GDPR in the EU, we should question whether voluntary regimes are appropriate in this area. Whereas the EU-Japan deal is silent on the action that should be taken, the EU submission to the WTO provides clear cover for a party to implement stringent data protection legislation. It provides that countries "may adopt and maintain the safeguards" including "the adoption and application of rules for the cross-border transfer of personal data". The USMCA specifically warns against applying any restrictions on cross-border flows of data unless they are "are necessary and proportionate to the risks presented."

One positive aspect to highlight is the inclusion of data protection as a specific provision, especially since it recognises the role that data protection regimes can play in increasing trust in digital trade. And although it is unlikely that this is how the US will use the provision, it does leave open, even under the USMCA and CPTPP text, for a state to adopt EU-style privacy and data protection rules.

The EU will not sacrifice its position on data protection, since this is part of the region's strategy to differentiate itself from the liberal free market approach of the US and the state capitalism of China. In order for the EU to be able to transfer personal data, its trade partner would need to pass an "adequacy test"[30] to ensure that the data would be protected. There is an interesting argument emerging that should the EU allow the US to insert the footnote mentioned above, which allows voluntary regimes to be sufficient to comply with the provision of the free trade agreement, then this could allow the US to argue that since they comply with their treaty obligations, their protections must be adequate and sufficient. This would represent a massive strategic victory for the US and fundamentally undermine the EU's data protection regime.

The other US strategy to ensure that minimal data protection rules can cooperate with jurisdictions with a high level of protection is contained within paragraph 5 of the provision. The section basically encourages states to mutually recognise each other's privacy and data protection rules, potentially even when they are in no way analogous in terms of impact on data protection. As the Electronic Freedom Foundation notes, what this means in reality is that places like the EU with higher personal data protection laws are strongly encouraged to treat data protections regimes like the US with its weak voluntary arrangements as equivalent enough to ensure that data can be collected, processed and transferred across borders.[31]

27 Arguably also China but none of the agreements analyses for this document involve China.
28 Laufer, W.S. (2013) *Social Accountability and Corporate Greenwashing*. Journal of Business Ethics 43, 253–261 (2003) doi:10.1023/A:1022962719299
29 Koehler, D. (2007) *The Effectiveness of Voluntary Environmental Programs—A Policy at a Crossroads?* Policy Studies Journal Vol 35, Issue 4
30 European Commission. *Adequacy Decisions*. Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
31 Malcom, J. & Maira, S. (2015, November 5) Release of the full TPP text after five years of secrecy confirms threats to users' rights. Electronic Frontier Foundation. Retrieved from https://www.eff.org/deeplinks/2015/11/release-full-tpp-text-after-five-years-secrecy-confirms-threats-users-rights

OPEN INTERNET ACCESS

CPTPP	EU-Japan	USMCA	EU Submission to WTO
Article 14.10: Principles on Access to and Use of the Internet for Electronic Commerce		Article 19.10: Principles on Access to and Use of the Internet for Digital Trade	2.9 Open Internet Access
Subject to applicable policies, laws and regulations, the Parties recognise the benefits of consumers in their territories having the ability to:		The Parties recognize that it is beneficial for consumers in their territories to be able to:	Subject to applicable policies, laws and regulations, Members should maintain or adopt appropriate measures to ensure that end-users in their territory are able to:
(a) access and use services and applications of a consumer's choice available on the Internet, subject to reasonable network management;		(a) access and use services and applications of a consumer's choice available on the Internet, subject to reasonable network management;	(a) access, distribute and use services and applications of their choice available on the Internet, subject to reasonable and non-discriminatory network management;
(b) connect the end-user devices of a consumer's choice to the Internet, provided that such devices do not harm the network; and		(b) connect the end-user devices of a consumer's choice to the Internet, provided that such devices do not harm the network; and	(b) connect devices of their choice to the Internet, provided that such devices do not harm the network; and
(c) access information on the network management practices of a consumer's Internet access service supplier.		(c) access information on the network management practices of a consumer's Internet access service supplier.	(c) have access to information on the network management practices of their Internet access service supplier.

The principle that the internet should be open access and non-discriminatory has been important to the development of the internet and the wider digital economy. The concept of "net neutrality", holds that "internet service providers (ISPs) must treat all internet communications equally, and not discriminate or charge differently based on user, content, website, platform, application, type of equipment, source address, destination address, or method of communication."[32] This principle has real impacts – in fact it is highly debatable whether services like Skype or Netflix would have been able to thrive and grow without being protected from having their traffic discriminated against without basic net neutrality principles.

Without net neutrality, ISPs could limit what you can and can't see. This is already the situation in many authoritarian regimes around the world where they attempt to actively control and manage what information is visible to their citizens and what services they can use. The fear is that were net neutrality to go, then certain content and services may be completely blocked by some ISPs, while they could also force websites to pay or suffer slow data transfer speeds, which might drive many smaller online services out of business.

The text in the trade agreements does not enshrine the principle of net neutrality but instead frames it as "principles on Access to and Use of the Internet for Electronic Commerce", in CPTPP and USMCA, with the EU simply referring to "open internet access". This importantly frames the provision as one that seeks to keep the internet as open as necessary rather that enshrining net neutrality as a concept.

There is no mention of open internet access in the EU-Japan deal. We should probably not read too much into this other than the fact that the issue was not important enough for either side to require its inclusion in the deal, nor were they able to easily agree on suitable wording that reflected their position accurately – since the EU already has both its own text and has signed free trade agreements containing such provisions.

The other three free trade agreements all share the same language with the only difference being that the CPTPP and EU submission to the WTO preface that the requirements are "subject to applicable policies, laws and regulations". The common text does not establish any enforceable obligation on states but instead focuses on ensuring that parties "recognise the benefits" of people and businesses having the ability to "access and use services and applications of a consumer's choice" and are able to "connect devices of their choice to the Internet" and "access

32 Wikipedia - https://en.wikipedia.org/wiki/Net_neutrality

information on the network management practices" of ISPs. There are small qualifications to these, such as only being able to connect a device if it does not harm the network.

There is an interesting subtle but important difference between the CPTPP and USMCA when compared with the EU submission to WTO. All texts state that "access and use services and applications of a consumer's choice" can be subject to "reasonable network management", which is a very broad term and leaves open the potential for ISP to implement traffic management policies. This text clearly opens the door for ISPs to start actively managing the traffic over their network in clear contravention of the principles of net neutrality. The EU adds a vitally important word to the provision, "non-discriminatory". This is omitted from the other treaties and provides a vital safeguard against discriminatory traffic management by ISPs – and therefore preserves some semblance of net neutrality. Overall, the provision on net neutrality provides no protection because it is so weak, especially in the US-led treaties. And even more damningly "it may actually impede the development of stronger, more meaningful global standards."[33]

Even though many already consider net neutrality to be dead in the US following the FCCs Restoring Internet Freedom Order made in 2017 and implemented in 2018 which gave ISPs a free hand "to do practically whatever they like",[34] in Europe, and much of the rest of the world, the fight is still ongoing – and it is a fight that really matters.

33 Malcom, J. & Maira, S. (2015, November 5) *Release of the full TPP text after five years of secrecy confirms threats to user's rights.* Electronic Frontier Foundation. Retrieved from https://www.eff.org/deeplinks/2015/11/release-full-tpp-text-after-five-years-secrecy-confirms-threats-users-rights
34 Kelly, M. (2018, June 11) *Net Neutrality is dead – what now? Retrieved from* https://www.theverge.com/2018/6/11/17439456/net-neutrality-dead-ajit-pai-fcc-internet

PRACTICAL IMPLICATIONS FOR LABOUR AND LABOUR MARKETS

The analysis contained in the previous section clearly shows that there are major concerns about critical areas of the digital economy having their rules set globally in the interests of developed countries and specifically the tech giants that operate in those countries. We have highlighted some of those issues within each provision. In this section, however, we want to look at how the entire digital trade chapter, within the context of the wider free trade agreement that it sits within, could impact on the world of labour and labour markets.

It is important to note that the practical implications that we go through are possibilities based on assumptions. We make these assumptions clear in each example where they are applied. Because the digital economy is still developing and because many countries are yet to sign up to digital trade agreements, there are many impacts that we are yet to see. Equally, it can also be the case that assumptions made about new areas of legal text can miss key practical implications that only come to light when tested by actual implementation and enforcement.

What is clear is that the tech giants are already having a material impact on the world of work – much of it very disruptive and directly affecting the lives of workers, particularly in less secure, less well-paid sectors of the labour market.

In many cases, as the analysis below suggests, what digital trade agreements are often doing is not creating additional problems, although that is sometimes the case. One example is the increased restrictions on source code sharing. Instead, they mostly contain provisions that benefit the tech giants most, like free cross-border flows of data or banning localisation requirements, enabling them to continue to benefit disproportionately from the digital economy. As Deborah James, director of Our World is Not for Sale, puts it, corporations "have long used trade agreements to lock in rules favoring their 'rights' to make profits, while limiting governments' ability to regulate them in the public interest, often in ways that could not advance through normal democratic channels."[35]

IMPLICATION 1 – INCREASE PRECARIOUS WORK

Technology is already disrupting labour markets everywhere, with future automation and the Fourth Industrial Revolution set to make the coming decades' disruption even more severe.[36] Although the tech giants have created some highly skilled jobs such as engineers, coders and product designers, the majority of new jobs created or multiplied by tech are precarious and low skilled. Examples of these types of work include delivery drivers at Hermes, cleaners on TaskRabbit or data entry at Amazon Mechanical Turk. These occupations generally see workers being defined as "self-employed" or "agency", denying them many employment rights.[37] The work often lacks fixed or predictable hours, which is the attraction to some, but makes it very hard to raise a family or get a mortgage. Ratings systems, overbearing surveillance and formal job targets disempower workers at the expense of employers and buyers. This is because low ratings or missed targets, even when unmerited or unattainable, can have serious consequences, including sanctions and loss of employment.

Key to the success of all these platforms is the huge amount of data that they collect and process together with their ambition to disrupt and dominate existing markets, often with little regard for existing regulation or the wider social impacts. Although the tech giants did not invent bogus self-employment or precarious work, they have extended its reach and in certain instances they have changed its nature in important ways. In Spain a recent report found that 17 per cent of people engaged in platform work.[38] As platform work proliferates, collective bargaining has been especially curtailed, since this is much harder for the self-employed. Meanwhile, both the breadth

35 James, D (2017 November 22) *Twelve reasons to oppose rules on digital commerce in the WTO.* Retrieved from https://www.huffpost.com/entry/twelve-reasons-to-oppose-rules-on-digital-commerce

36 Manyika, J et al (2017) *Jobs Lost, jobs gained: Workforce transitions in times of automation.* Mckinsey Global Institute. Retrieved from https://www.mckinsey.com/featured-insights/future-of-work/jobs-lost-jobs-gained-what-the-future-of-work-will-mean-for-jobs-skills-and-wages

37 Eurofound (2018) *Platform work: Employment status, employment rights and social protection.* Retrieved from https://www.eurofound.europa.eu/data/platform-economy/dossiers/employment-status

38 Caniqueral, A. (2019, June 30) *How can tech meet the needs of platform workers?* Retrieved from https://www.thersa.org/discover/publications-and-articles/rsa-blogs/2019/06/tech-platform-workers

and depth of worker surveillance has been extended significantly, with examples including logging employee keystrokes on their keyboards, currently done by 45 per cent of American companies,[39] to requiring employees to wear tracking devices, 202 million of which were handed out in 2016,[40] to using specialist software to monitor staff social media and private messaging apps.[41]

Many tech giants, such as Uber[42] or Foxconn[43], have an explicit goal to automate as much of their labour as possible, investing billions to make it happen. Key to making it happen are the workers who provide the data required to build the algorithms to replace them. The nature of these data-driven digital markets is that the company with the largest data trove and the ability to process it into actionable intelligence has a real competitive advantage.[44]

Many of the e-commerce provisions analysed in this report, including the prohibition on data localisation, source code secrecy, free cross-border data flows and the abolition of net neutrality, all favour the largest transnational tech companies because they exploit opportunities of scale, benefit most by keeping source code secret, are best able to exploit global data flows and meet the costs of a non-neutral internet. These data flows, as well as the code and insights built from the data, will become ever more important in the future as we see more and more jobs automated and platformatised. This will make it much harder for local and non-digital alternatives to survive or emerge, especially ones with different social or environmental considerations. In the absence of a change in employment model among tech giants, this is likely to lead to an increase in the number of people who are forced to work under the conditions associated with platformatised work.

IMPLICATION 2 – MAKING ENFORCEMENT OF LOCAL LABOUR LAWS MORE DIFFICULT

When a law is broken, an entity must be brought to court to answer the charge. A company having a locally registered entity makes this process easy because they can be legally compelled to engage with the domestic legal process and comply with its judgements. On the other hand, as the ITUC has previously commented: "without a local presence of companies, there is no entity to sue and the ability of domestic courts to enforce labour standards, as well as other rights, is fundamentally challenged."

The latest EU Submission to the WTO for telecom services is already proposing that providers of services should not be required to establish a local legal entity. The influential Cato Institute say their ideal UK/US trade agreement would "forbid any 'local presence' requirements, conditions that require service suppliers of another party to have an office or store or any form of presence."[45] As more and more services become mediated through platforms, and the internet enables us to exchange goods, services and information with anyone, we need to ensure that we maintain our ability to enforce domestic laws as appropriate, including labour laws.

The erosion of our ability to enforce domestic legislation is not a theoretical possibility but one which is already happening, facilitated by the internet and digital technology and global trade. There are already examples of this happening on a small scale with certain services, like online tutoring. In this sector, it is quite easy to contract a person resident in your country but working for a platform, or an agency based in another country, to tutor you. In some instances the company that you contract the work through will have no legal entity established in your country. This means that it will be hard for those purchasing the service to hold the company to account for failing to properly deliver the service or other issue requiring a legal remedy.

If this were extended to major gig-economy companies such as Uber and they were not required to have a local legal entity, it would become very difficult to enforce domestic labour laws and workers' rights, as is currently the experience of many countries trying to enforce labour laws against platforms with a local presence. If enforcement were compromised in this way, the authority's only option would be to enforce against the drivers themselves, since they are a legal entity located in the country. However, the authorities would find it almost impossible to enforce anything because most employment rights, from minimum wage to sick pay, do not apply to self-employed contractors. It is therefore vital that, in order to ensure that labour law can be enforced locally, any company

39 McCann, D. & Warin, R. (2018) Who Watches the Worker? New Economics Foundation. Retrieved from https://neweconomics.org/2018/06/who-watches-the-workers
40 Wild, J. (2017, February 28) *Wearables in the workplace and the dangers of staff surveillance*. The Financial Times. Retrieved from https://www.ft.com/content/089c0d00-d739-11e6-944b-e7eb37a6aa8e
41 Solon, O. (2017, November 6) *Big Brother isn't just watching: workplace surveillance can track your every move*. The Guardian. Retrieved from https://www.theguardian.com/world/2017/nov/06/workplace-surveillance-big-brother-technology
42 Newton, C. (2014, May 28) *Uber will eventually replace all its drivers with self-driving cars*. The Verge. Retrieved from https://www.theverge.com/2014/5/28/5758734/uber-will-eventually-replace-all-its-drivers-with-self-driving-cars
43 Javelosa, J. (2017, Jan 3) *Apple manufacturer Foxconn to fully replace humans with robots*. Retrieved from https://futurism.com/apple-manufacturer-foxconn-to-fully-replace-humans-with-robots
44 Mayer-Schonberger, V. & Ramge, T. (2018) Reinventing Capitalism. John Murray
45 Ikenson, D., Lester, S. & Hannan, D. (2019) The Ideal US-UK Free Trade Agreement. Cato Institute. Retrieved from www.ifreetrade.org/pdfs/US-UK-FTA.pdf

that employs people in a country must have a legal entity in that country. This will ensure that labour laws are there to protect everyone and that companies are held to account for their behaviour towards their workers.

IMPLICATION 3 – ERODING WORKERS' RIGHTS BY NECESSITY

The labour market consists of a balance between different forces, and workers usually need to fight hard for their rights (relative to companies and owners of companies) to be enshrined in law. Ending child labour or creating the five-day week did not happen thanks to the generosity of business, but rather the concerted effort of workers, unions and civil society – and usually against the odds – ultimately implemented by democratically accountable governments. The digital transformation that society is undergoing is testing some of those hard-won rights about what constitutes a worker and what rights and protections they deserve.

Most provisions in trade agreements contain exemptions that allow governments to regulate in an area that would otherwise be prohibited by the free trade agreement. These derogations are often further qualified by the fact that they should meet a "legitimate public policy objective" and that it is "no more restrictive than necessary", known as the necessity test.

It is important to acknowledge that the test has evolved incrementally over time as the WTO Appellate Body has ruled on cases. An early example involved the banning in California of a petrol additive that was polluting water supplies. However, a Canadian supplier of the additive claimed this failed the necessity test because in theory California could have solved the problem by requiring all storage tanks to be dug up and resealed properly. The WTO held in favour of the Canadian company because they had indeed proposed something that was less restrictive on global trade. This early jurisprudence was criticised for being too biased towards trade.[46] Although the jurisprudence has moved a little, it remains very hard for parties to meet the legitimate necessity tests for certain derogations.

When considered in the abstract, the necessity test can seem to be quite reasonable. But as the excellent example laid out by Laura Bannister, senior adviser at the Trade Justice Movement, at the recent WTO Public Forum about worker surveillance shows, this could become problematic.[47] Many gig economy workers are already under heavy surveillance at work, and this is currently expanding to cover non-working hours as well.[48] Already, workers and trade unions are demanding new digital rights for workers and an end to excessive digital surveillance. Should they be successful in their demands and the government enact policy that banned or severely curtailed the ability of companies to collect data based on excessive surveillance, it could be considered "more restrictive than necessary" by a trade court. This is because the tech company would be able to show an impact on its ability to trade, but the unions and workers may struggle to prove scientifically or beyond doubt that the surveillance and data gathering was damaging to workers' well-being or their privacy. Other areas that are critical to workers and unions could also have problems when set against the necessity test such as workers' privacy, data security or common data ownership.

IMPLICATION 4 – CHALLENGES TO ALGORITHMIC TRANSPARENCY

Algorithms are not new, but thanks to the digital revolution, they are becoming a part of an ever-increasing portion of our lives. They are indispensable in the online world due to the need to sort huge volumes of information in order to make the internet the valuable service it is today. As the digital economy has grown, the reach of algorithms has extended. Today they are responsible for almost 40 per cent of stock trades in the UK. They fly planes for over 95 per cent of the time the planes are in the air. And they may soon be driving our cars. Algorithms are also expanding into new areas to help people make decisions about whether to offer an applicant a job interview, whether offenders will reoffend, and what social care provision a service user needs. Despite presenting a technological veneer of objectivity around their decisions, algorithms, and the data collection that powers them, are designed by people, and their parameters and foundational assumptions are shaped by ultimately subjective human decisions.

As algorithms enter increasingly sensitive areas of our lives, we need to have meaningful accountability for those who create and deploy algorithmic decision systems, especially in areas where decisions have a significant impact on individuals.

The source code provisions in emerging e-commerce deals would make it very difficult for governments to require access to source code as a condition of market

46 Howse, R. (2002) *Human Rights in the WTO: Whose Rights? What Humanity? Comments on Petersmann.* 13 EJIL 651, p. 657.
47 Audio recording of WTO Public Forum Session 129. Retrieved from https://www.wto.org/audio/pf19session129.mp3
48 McCann, D. & Warin, R. (2018) *Who Watches the Worker?* New Economics Foundation. Retrieved from https://neweconomics.org/2018/06/who-watches-the-workers

access. The limitation to defined legal areas such as intellectual property or competition could make it very hard to require access in order to meet transparency, accountability and auditing requirements of future algorithmic accountability systems.

The source code provisions would make it hard for workers to examine the internal workings of the algorithms that will become central to the world of work. Algorithms are already being used in a wide range of areas within work, with one of the highest profiles being around hiring algorithms. Algorithmic systems review CVs and online applications to select the most suitable candidates in order to automate some, or all, of the recruitment process. In 2018 Amazon decided to abandon its own hiring algorithm that it had been developing for four years because it "realized its new system was not rating in a gender-neutral way."[49] If Amazon with its deep pockets and strong AI developer base could not rectify for the biases of the algorithm, one has to question whether the many commercial sellers of such software have been able to do so.

In order to be able to have more transparency and understanding of the actual performance of these critical source codes, AI ethics advocates want algorithms to be made visible enough to inspect and understand them, particularly when they lead to decisions that have questionable or negative consequences, such as a job application denial or a driverless vehicle accident. This could be made very hard, or impossible, with the current prohibitions on source code disclosure requirements in FTAs. Indeed, as award-winning journalist Kate Kaye puts it, "The push to restrict access to algorithms doesn't work for people, it doesn't work for users, it doesn't work for consumers."[50]

IMPLICATION 5 – EXPANDING MARKET ACCESS RIGHT FOR DIGITAL FIRMS

There is a quiet revolution going on within government, known as Gov Tech, that could transform the nature of public services and who delivers them, because automated decision systems are being increasingly used to decide who should receive them as well as systems to target "most efficiently" the scarce resources. Mimicking other tech-based disruptions like fintech[51] or proptech[52], a recent PriceWaterhouseCooper report argued that "Gov Tech has the power to transform the delivery of public services, achieve better for less and improve the user experience."[53]

We are already seeing technology companies getting into the heart of key decisions that we normally associate with the state. Examples include predictive algorithms, which give police suggestions for which areas to focus their increasingly limited resources on,[54] and software attempting to predict whether a newborn child will be subject to abuse in the future.[55]

As public service delivery increasingly relies on digital algorithms and data, this could also mean an increased role for the private sector in core areas of public services. The additional challenge that the e-commerce rules may introduce is the limitation of government control and regulation over companies that will be delivering key public services. E-commerce rules could mean that governments will not be able to demand the source code by default, nor limit the flow of data, nor require any of the data collection and analysis to be conducted locally. Demanding the source code is vital in order to ensure that the systems function as per the specifications and design of the system as well as to ensure that it is not biased against certain sections of the population. Equally, limiting the flow of data is vital, since some of the data will be highly sensitive, such as health or police data, and it will therefore not be appropriate for the data to be transferred internationally by default, thereby losing jurisdictional control and access to it.

An additional challenge is that the digitalisation of public services is also being used as a tool to increase and lock in the range or public services that could be delivered by the private sector to areas such as health care, education, local government, electricity and water distribution, by tech firms trying to expand their "market access" rights. For example, Uber, which ultimately wants to operate a single mobility platform with as much automation as possible, has acknowledged its intention to table proposals that would expand the "market access" rights for digital firms in sectors under WTO rules. Uber also wants to expand the scope and coverage of those sectors,

49 Dastin, J. (2018, October 10) *Amazon scraps secret AI recruiting tool that showed bias against women.* Retrieved from https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idI

50 **Kaye, K. (2018, November 8) *How the tech industry coordinated to squelch algorithm transparency in the new NAFTA deal.* Retrieved from** https://redtailmedia.org/2018/11/08/how-the-tech-industry-prevented-algorithm-transparency-in-nafta-2-0/

51 Term for a business that is applying technology in order to deliver financial services industry

52 Term for a business that is applying technology in order to deliver property services, especially rentals

53 PriceWaterhouseCooper. *GovTech: the power to transform public services in the UK.* Retrieved from https://www.pwc.co.uk/industries/government-public-sector/gov-tech.html

54 Couchman, H. (2019) *Policing by Machine.* Retrieved from https://www.libertyhumanrights.org.uk/sites/default/files/LIB%2011%20Predictive%20Policing%20Report%20WEB.pdf

55 Pegg, D. & McIntyre, N. (2018 September 16) *Child abuse algorithms: from science fiction to cost-cutting.* Retrieved from https://www.theguardian.com/society/2018/sep/16/child-abuse-algorithms-from-science-fiction-to-cost-cutting-reality

which could open up many more public services to the threat of privatisation, even potentially against the express will of the people and government.

Increased privatisation by tech firms could leave important public services in the hands of digital corporations with weak accountability and obligations to local communities for ensuring quality and accessibility of service.

IMPLICATION 6 - INCREASE POWER OF BIG TECH OVER WORKERS

The introduction of data-gathering technology, its analysis and use has disrupted the delicate balance between worker and employer, and has shifted power firmly back to employers. This is especially true within the new labour platforms like Deliveroo or Amazon Mechanical Turk but is now filtering into all areas of work. A recent report by the New Economics Foundation found that companies were increasing their power over employees in a number of ways.[56] Firstly, by extending their surveillance of them temporally, beyond the core hours of work, and spatially, to include surveillance of the body itself. Incredibly, 45 per cent of US companies currently log key strokes of their workers.[57] Secondly, because the company owns the data that is produced, it is overwhelmingly used for the benefit of management, leading to an increased workload for each worker and, when there is no opportunity to use the increase in work to produce more, a reduction of employees. The poster child for work intensification is Amazon, which through compulsive monitoring and stringent targets, ensures that all its workers' activities are tracked, recorded, and assessed to ensure they meet exacting targets at all times. Thirdly, employers are hiding behind algorithmic decision systems that affect workers, materially leading to loss of accountability and the potential to entrench biases.

These developments are already seeing the power of workers reduced in favour of employers. Digital trade agreements did not create these issues but they do limit the policy space of countries so that it can be hard to mitigate for these negative outcomes. There are three provisions within the digital chapters of trade agreements that enable Big Tech to increase and cement their position of power over workers. Firstly, the unregulated cross-border transfer of data will ensure that Big Tech is able to acquire all of the data that it needs to surveil its workforce while careful analysis of the data helps the companies get the most out of their workers. Secondly, the provision to ensure that source code cannot easily be accessed, especially for issues of bias or discrimination, will allow companies to continue to hide behind the "black box" algorithms that they deploy. Finally, the application of the necessity test may act to limit the potential for workers to fight back against intrusive data gathering practices by a company.

As we noted in the example devoted to the necessity test, this could limit the ability of workers and their unions to resist intrusive surveillance and monitoring. This is especially worrying given that we are now seeing cases of people dismissed for behaviour outside the workplace and outside of work hours. It is projected that by 2021 over 500 million employees will be monitored through wearable technology. Companies are using data to develop the digital intelligence to control and manage the remaining workforce even more closely, leading to an ever-increasing cycle of intrusion and surveillance.

The provisions around source code threaten to allow employers to hide behind automated decision-making systems, thereby reducing their accountability. Key decisions about whether to hire someone and who to fire are now frequently made by algorithms. Without getting access to the source code, it may be very hard to ascertain whether the system is functioning correctly or whether the system is discriminatory against certain sections of the population.

IMPLICATION 7 - THREATEN COUNTRIES' DOMESTIC INDUSTRIES' FUTURE BY REQUIRING THE FREE TRANSFER OF THE DATA

From some perspectives it is incredible that the modern tech companies are some of the most valuable companies in the world, especially given the fact that many of them, like Google or Facebook, offer a product that is free to use, while others, like Uber or Spotify, still fail to make a profit. What lies behind the valuations are the incredibly large data troves that they have gathered during the course of their operations and that are central to their success and dominance. All tech companies rely on and benefit from the ability to gather large amounts of data from users and workers within their ecosystem, often supplemented by data sets purchased from third parties. Their engineers build sophisticated algorithms to analyse the data and turn it into actionable intelligence, which they can in turn monetise to generate revenues and profits. Probably one of the best examples to illustrate the point is Uber. Uber is a transportation company that is currently valued at about $50bn yet owns no cars and employs no drivers and continues to makes

56 McCann, D. & Warin, R. (2018) *Who Watches the Worker?* New Economics Foundation. Retrieved from https://neweconomics.org/2018/06/who-watches-the-workers
57 Johnson, C. (2017) *Meeting the Ethical Challenges of Leadership: Casting Light or Shadow.* SAGE Publications Inc.

huge losses.[58] Uber lost a staggering $5.24 billion in the second quarter of 2019.[59] What Uber lacks in terms of capital and infrastructure it makes up for by gathering and analysing an immense volume of data on people, drivers and their cars and how they move around the city and interact with each other. This data not only allows it to refine and improve the service that it offers customers today, in the future it will allow Uber to achieve its ultimate aim of being a transportation company without drivers at all, since the data is being used to build self-driving cars which will ultimately replace its entire fleet. Although not specifically linked to the digital chapter provisions of trade deals, Uber has recently signalled its intention to sue Colombia for banning it from the local market – something which may only become more common when digital chapters are more widely included in trade deals.[60]

It hard to see why, given the circumstances outlined above, countries should be precluded from implementing policies and laws that would enable them to develop their own domestic tech industry by placing limits on the flow of data out of the country or requiring the localisation of servers and people. Just as Norway did with oil extraction technology[61] or South Korea did with consumer technology[62], it is vital that countries have the tools to impose conditions on companies operating domestically that will foster a new generation of businesses along with new jobs.

This is especially the case because in the future the success of businesses in many sectors will be rooted in their ability to collect and analyse data. If a large part of the data is being gathered by transnational platforms who are able to aggregate global data streams, thanks to the liberal and free cross-border flow of data, then it will be much harder for domestic competitors to emerge, since, even if they have the capital to employ the people and data analytics systems, they will never be able to match the quantity of data.

IMPLICATION 8 - PREFERENCING TRANSNATIONAL COMPANIES OVER MICRO, SMALL AND MEDIUM ENTERPRISES (MSME)

One of the main publicly stated rationales for pursuing e-commerce and now digital trade provisions in free trade agreements is to enable and empower MSMEs to be able to trade digitally and therefore open up markets that would previously only been available to large multinationals. Completely reformulated rules, written by and for MSMEs, could deliver on this noble sentiment and provide real opportunities for them to grow and reach wider markets. However, in reality, the proposals and signed agreements will do little or nothing to help MSMEs, and in fact they are very much aligned with the needs of Big Tech companies, who would undoubtedly benefit the most. In addition, the way that the digital economy operates more generally also favours the tech giants over MSMEs.

MSMEs are the real engine of the economy, not just in developing countries but in developed ones too. They generally account for the majority of employment, accounting for as much as 45 per cent of jobs, as well as economic activity, an average of 33 per cent of national income.[63] However the demands of Big Tech, which are promoted by a growing army of lobbyists, are often at odds with the needs of MSMEs. A pertinent example is with regard to tax payments. Tech giants exploit their global presence to ensure that they minimise their tax liability which leads to situations in which Apple's Irish subsidiary pays just 0.0005 per cent tax in 2014.[64] Equally, Uber in the UK routes all its customer payments through Luxembourg, therefore avoiding VAT in the UK, although this is being taken through the courts.[65] This makes it very hard for any MSME to compete, since they are unable to avail themselves of complex legal structures and therefore find themselves at a 20 per cent cost disadvantage.

The combination of several of the provisions could be additional barriers preventing MSME emerging and competing against the established tech giants while at the same time specifically being advantageous to the tech giants. For instance, MSMEs would benefit much less than Big Tech from the cross-border free

58 Palmer, A. (2019, October 1) *Uber and Lyft close to record lows as investor skepticism grows around recent IPO*. Retrieved from https://www.cnbc.com/2019/10/01/uber-closes-at-record-low-worth-less-than-50-billion.html
59 Clark, K. (2019, August 8) *Uber lost more than $5B last quarter*. Retrieved from https://techcrunch.com/2019/08/08/uber-stock-plummets-following-second-quarter-earnings-report/
60 Griffin, O. (2020, January 10) *Uber to take exit ramp in Colombia after 'arbitrary' court ruling*. Retrieved from https://www.reuters.com/article/us-uber-colombia/uber-to-take-exit-ramp-in-colombia-after-arbitrary-court-ruling-idUSKBN1Z921L
61 Heum, P. (2008) *Local Content Development: experience from oil and gas activities in Norway*. Institute for research in economics and business administration. Retrieved from https://openaccess.nhh.no/nhh-xmlui/bitstream/handle/11250/166156/A02_08.pdf?sequence=1
62 Chen, C. & Sewell, G. (1996) *Strategies for technological development in South Korea and Taiwan: the case of semiconductors*. Research Policy Volume 25, Issue 5, Pages 759-783. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/0048733395008616
63 OECD (2017) *Enhancing the Contributions of SMEs in a Global and Digitalised Economy*. Retrieved from https://www.oecd.org/industry/C-MIN-2017-8-EN.pdf
64 Taylor, H. (2016 August 30) *How Apple managed to pay a 0.005 percent tax rate in 2014*. Retrieved from https://www.cnbc.com/2016/08/30/how-apples-irish-subsidiaries-paid-a-0005-percent-tax-rate-in-2014.html
65 Kaminski, I. (2019 October 10) *Uber's VAT liability confirmed*. Retrieved from https://italphaville.ft.com/2019/10/09/1570629132000/Uber-s-UK-VAT-liability-confirmed/

flow of data because they are much less likely to need the provision to run their operations, since MSMEs are overwhelming based in one country. MSMEs would also be less likely to take advantage of buying large data sets that had been assembled thanks to moving data transnationally. In addition, since digital services can be improved by the analysis of large datasets, the liberal free movement of data across borders will preference Big Tech corporations.

MSMEs have raised very specific concerns about the market concentration of Big Tech players in many sectors that are critical for e-commerce, such as marketplaces, electronic payment solutions and logistics providers. MSMEs also complain that companies operating in these concentrated marketplaces are able to exploit their position to charge excessive fees and membership. These concentrated markets mean that MSMEs, with their limited bargaining power, are at the mercy of these companies, because if they want to participate in the global e-commerce market, they need to use these services, even if the terms feel unfair. The rise of this dynamic has led to a resurgence in interest around the concept of monopsony, the less well-known cousin of monopoly. Whereas "monopoly" is defined as "a market structure characterised by a single seller, selling a unique product in the market", "monopsony" on the other hand describes "a market situation in which there is only one buyer".

As Richard Hill, prominent civil society activist, noted: "While the concept of e-commerce is good for SMEs, the actual e-commerce rules being proposed at the WTO would enable the platforms whose dominance is already a problem for SMEs to further squeeze SMEs to pay them more." As more and more purchases are made online and physical shops close down at ever-increasing rates, this poses a serious challenge to the tax receipts, especially for local government, which is often very reliant on local business property taxes for its revenue.

IMPLICATION 9 – AGRICULTURE AND DIGITAL TRADE

Global agriculture and the wider food system is undergoing a revolution that may well be as dramatic as any previous one. There have been three major revolutions, starting with the original agricultural revolution of the 18/19th century Europe, followed by the green revolution of the 1950s and 60s, and finally the GMO revolution of the 2000s. Today, the prospect of workerless farms staffed by robots is on the horizon, with many working on it[66] while others are already doing it (at huge cost).[67] Mass adoption, however, remains a distant prospect, for now. Instead, what is happening today is a radical restructuring of how, and by whom, our food is produced and distributed. Globally the small-scale food system, where (often family) farmers grow on small plots, often using traditional methods and selling their own produce directly in physical markets or on the streets, still feeds 70 per cent of people around the world.[68] In recent years, just as traditional methods of farming have been challenged, traditional markets have been facing increased competition from online marketplaces. This transition has the potential to inflict hardship on millions as their livelihood becomes a sector driven by big data, technology and global companies.

The advance of Big Tech companies into agriculture and the wider food system presents a number of challenges to those trying to make a living, and feed themselves, from small-scale agriculture. A growing concern is that new digital technologies, which allow genes to be assembled in a lab, allow new forms of bio-piracy that bypass existing regulations to the detriment of local and indigenous communities.[69] This will transfer a valuable asset from the commons, to be used by all farmers, to something owned and controlled by the agritech sector. The behaviour of companies like Monsanto, which came to prominence in the third agricultural revolution, in developing terminator seeds so farmers can't save seeds while taking those who do to court, is stoking this fear. In addition, as the process of growing food becomes ever more reliant on technology, from growing, to harvesting, to distributing, technology companies from outside the agricultural sector, such as Fujitsu and Amazon, are increasingly buying existing companies with the potential to further dominate the agritech sector.[70]And as with all data-driven businesses, the fear is also that over time these large companies will coalesce into an even smaller number of mega companies, as is already the case in many sectors of agriculture today.[71]

More and more food is now being delivered over digital platforms rather than physical markets and shops. The platformisation of the food delivery system is not only calling farmers' livelihoods into question but is also creating a more general problem of regulation and accountability. For instance, Alibaba,

66 Paquette, D. (2019 February 17) *Farmworker vs Robot.* Retrieved from https://www.washingtonpost.com/news/national/wp/2019/02/17/feature/inside-the-race-to-replace-farmworkers-with-robots/
67 Thu, M. & Hong, B. (2016 March 24) *Smart farming a bright future for Vietnam.* Retrieved from https://www.nationthailand.com/business/30282386
68 ETC (2017) *Who will feed us? Industrial food chain vs the peasant food web.* ETC Group. Retrieved from https://www.etcgroup.org/content/who-will-feed-us-industrial-food-chain-vs-peasant-food-web
69 Servick, K. (2016 November 17) *Rise of digital DNA raises biopiracy fears.* Retrieved from https://www.sciencemag.org/news/2016/11/rise-digital-dna-raises-biopiracy-fears
70 Fujitsu website. *IoT in Agriculture.* Retrieved from https://www.fujitsu.com/global/themes/internet-of-things/hyperconnected-business/agriculture/
71 ETC (2018) *Too big to feed: the short report.* ETC Group. Retrieved from https://www.etcgroup.org/content/too-big-feed-short-report

a massive Chinese e-commerce platform, delivers fresh milk via its platform, often imported, directly to consumers in China (and other countries). Given that relatively few countries have existing regulations that adequately deal with the distribution of food online, especially when cross border, including vitally important standards around food safety, the development on international e-commerce channels for fresh food poses serious challenges.[72] For instance, who should be held responsible for issues related to the quality of the milk, how it is produced and ultimately who should be liable for problems that arise? This will be made even more complicated if the proposals in the new wave of trade agreements are implemented which would make it legal for a service supplier like Alibaba, or other e-commerce platform, to operate without a "local presence" in its country or, for example, to avoid a requirement to source food from local producers.[73]

A third challenge to small-scale farming, driven by Big Tech, is the level of vertical and horizontal integration of the agritech sector that we are seeing. An illustrative example is the acquisition by Monsanto of the digital agriculture and insurance company The Climate Corporation for nearly a billion dollars.[74] The huge value to Monsanto in the acquisition was the massive amount of data on farmers, crops and the climate along with the ability to turn the data into actionable intelligence, telling the farmer which seeds to plant, how much nitrogen to use or which pesticide to apply. While for many farmers this is useful information, few of them realise that the data they provide is much more valuable to the tech company, which uses it to target them with marketing and often aiming to eventually automate away their livelihood using the data together with "advancements in computing power, dexterity, motion planning, and computer vision which are enabling a new generation of robot."[75] The provisions cementing the international free flow of data will make it easier for multinational agritech businesses to harvest and compile data from around the world. This will allow them to generate better products, since they will have more data, than those that could be developed, either locally by farmers using their own data, or even by attempting to aggregate data nationally. In addition, the prohibition on requiring the sharing the source code of the software that will be increasingly essential for farms to use, even under technology transfer programmes, will act to protect the interests of multinational agritech at the expense of empowering local farmers and fostering a domestic industry.

The growth of a new generation of agri-businesses, powered by data and acquisition, seeking to enclose information (rather than land) such as seeds, DNA, or data about land and the efficacy of pesticide use, while marketing ever more sophisticated "precision agriculture",[76] is taking over our food system. This ensures that farmers are increasingly reliant on a few large multinational companies, which, through their use of precision agriculture technology, can minimise the use of inputs, such as water and pesticides, while maximising the outputs. This is compounded by the reliance that many already face on the likes of Monsanto for seeds and fertilizer. This can be seen as providing a solution to climate change for the agricultural sector,[77] but precision agriculture technology is extremely expensive, so only the largest companies can afford it. This change will make the livelihood of small-scale farmers even more precarious as they are unable to obtain the latest precision technology, and unfairly blamed for the climate crisis.

Historically, the agribusiness lobby has been critical of food and agriculture being excluded from bilateral Free Trade Agreements (FTAs).[78] Now not only do many FTAs include the agricultural sector, but FTAs are also often used to try to force open markets or constrain the power of governments to set their own regulatory standards. At the same time, the power of large-scale tech-driven agribusinesses is being advanced through the TRIPS intellectual property provisions through the WTO, which protect specific forms of intellectual property and facilitate mergers.

Even though the digital trade provisions are not creating the underlying issues, the liberal free flow of data linked to the prohibition on requiring source code transfer (as well as issues around local presence) means that large agritech businesses will continue to be benefit most at the expense of small-scale farmer.

72 GRAIN (2018 May 31) *Top e-commerce companies move into retail*. Retrieved from https://www.grain.org/en/article/5957-top-e-commerce-companies-move-into-retail
73 See Implication 2 – Difficulty enforcing local labour law
74 Tsotsis, A. (2013 October 2) *Monsanto buys weather big data company climate corporation for around $1.1B*. Retrieved from https://techcrunch.com/2013/10/02/monsanto-to-acquires-weather-big-data-company-climate-corporation-for-930m/
75 Alexander, B. (2018 October 3) *If farms are to survive, we need to think about them as tech companies*. Retrieved from https://qz.com/1383635/if-farms-are-to-survive-we-need-to-think-about-them-as-tech-companies/
76 NESTA website. *Precision Agriculture*. Retrieved from https://www.nesta.org.uk/feature/precision-agriculture/
77 Klein, A. (2019 July 26) *How tech is helping the agriculture sector curb carbon emissions*. Retrieved from https://www.weforum.org/agenda/2019/07/agtech-can-climate-proof-the-planets-harvests/
78 Bilaterals webpage. *Agriculture and Food*. Retrieved from https://www.bilaterals.org/?-agriculture-food-

PUBLIC SERVICES INTERNATIONAL
The global union federation of workers in public services

FRIEDRICH EBERT STIFTUNG

ENGLISH

Digital trade rules and big tech:

SURRENDERING PUBLIC GOOD TO PRIVATE POWER

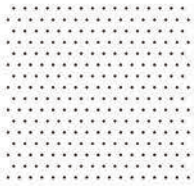
CONTENTS

Digital trade rules and Big Tech:
SURRENDERING PUBLIC GOOD TO PRIVATE POWER

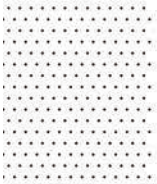
Written by Professor Jane Kelsey, Faculty of Law, The University of Auckland, New Zealand, with research support from Mary Ann Manahan, and peer reviewed by Dr Bill Rosenberg.

ABBREVIATIONS

AI	Artificial intelligence
AIIB	Asian Infrastructure Investment Bank
D2D	Digital 2 Dozen principles
FTA	Free trade agreement
GAFA	Google, Amazon, Facebook, Apple
GATS	General Agreement on Trade in Services
IoT	Internet of Things
IT	Information technology
PPP	Public Private Partnerships
R&D	Research and development
SOE	State-owned enterprise
SPV	Special Purpose Vehicle
TPPA	Trans-Pacific Partnership Agreement
USTR	United States Trade Representative
WTO	World Trade Organization



OVERVIEW



Big Tech companies like Google, Amazon, Facebook and Apple – GAFA for short - are using free trade agreements to protect themselves from regulation. The idea of a 'free and open' Internet sounds liberating. But a world in which powerful and unregulated private corporations control the digital domain on which everyone, from governments to families, has come to depend is the ultimate in privatisation

Digital technologies are becoming addictive. The Internet and its apps, social media, web searches, ride-shares and on-line market-places can now organise almost every aspect of our daily lives, all seemingly for free. But every time we use them, we generate more data that allows the shadowy corporations who control them to analyse our activities, opinions and friendships. Whether it's the US tech giants or their Chinese counterparts of Baidu, WeChat, Alibaba and Tencent, this new generation of transnational corporations is reaching ever-deeper into our lives.

Their power extends to the core of central and local government and public services. They monitor our workplaces, streets and even devices in our homes, and run our transport, telecommunications and energy infrastructure, sometimes from outside the country. They create the algorithms that decide who gets a job or gets fired, is given a loan or enters university, and the artificial intelligence that does the work of doctors, technicians and prison officers. Private contractors run the IT operations and data bases of government agencies, storing our data on their own servers or in the 'cloud', which usually means they are controlled in the United States. This list expands every week, as governments become more dependent on digital technologies and on the firms that control the information and systems that run them.

Every week, there is more evidence of how this power is being abused through tax evasion, breaches of human rights by profiling of immigrants and dissidents, and exploitating so-called 'self-employed' workers. Big Tech show no sense of responsibility or culpability for frauds on consumers, mass breaches of data privacy, or even the online hosting of extremism and the manipulation of democratic elections.

The last thing the state should be doing is surrendering its right to regulate these technologies and their owners. Governments are in a perpetual state of catch-up, trying to understand and respond to existing digital technologies and services only to see new, previously inconceivable ones emerge. There is currently very little regulation to control these activities or hold the tech giants to account. Their global reach allows them to organise their corporate identities, locations and operations to bypass the limited laws and restrictions, and

tax obligations, that do exist. Big Tech wants to keep it that way. That is the purpose of the new rules on 'electronic commerce' or 'digital trade' that their governments are securing for them through international free trade agreements. The Trans-Pacific Partnership Agreement (TPPA) set the template for later negotiations. Now there is pressure to adopt them in the World Trade Organization (WTO) and apply them on a global scale.

These rules have been negotiated under the radar. Governments seem bedazzled by unsubstantiated claims that adopting them will bring new development opportunities and potential cost savings, when in reality these rules are designed to tie their hands. Few trade officials really understand the implications of what they are negotiating. Few people outside those negotiations have been aware that these rules were being developed because of the secrecy that screens them from public view.

This report raises the alarm for public services unions in the Asia Pacific. These agreements will affect you in fundamental ways, as the public sector workforce, as users of public services, and as citizens. The first section sets out the Tech lobby's wish list and how that translated into the TPPA rules.

Section Two selects a number of issues of concern for PSI that are directly affected by the 'trade' rules: privatisation of public services, corporate control, data, digital technologies, source codes, public infrastructure, employment, working conditions, unionisation, public finance and social wellbeing. The third section examines the impacts in more detail with reference to healthcare and smart cities. The report concludes with some recommendations.

Hopefully, this will provide a platform for PSI affiliates to mobilise your powerful voices to stop the spread of the e-commerce rules, alongside other neoliberal trade and investment rules, and demand a progressive, people-centred alternative.

1. Key Impacts of Digitisation on Public Services

Cheerleaders of the 4th industrial revolution celebrate it as the next phase after the (failed) neoliberal mode of financialised capitalism. Unions have recognised the potential benefits of a digitised economy, but only with a commitment to a just transition that protects the rights of working people and enhances their well-being[1]. That is not the present model. The current trajectory, fuelled by the new e-commerce or digital trade rules, will have a radical and disruptive impact on public services, on public sector workers and unions, and on citizens, families and communities.

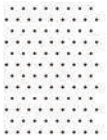
The recent report for PSI on Digitalisation and Public Services has analysed these challenges in depth[2]. The following selection of issues provides the framework for the case studies in this report on healthcare and 'Smart Cities'.

- **Privatisation of public services:** The neoliberal market-driven agenda says the state should only do what the private sector can't and what remains in the public sphere should be modelled on the private sector, including the drivers of efficiency, productivity, labour replacement and lowering labour costs. At the same time, most governments claim an ongoing commitment to improved services to the public with public service at its core. There is an illusion that digitisation enables a government to do both. Where a government tries, and discovers it can't, the 'e-commerce' trade rules will disable the government from re-regulating data, digital technologies and services in ways that prioritise the public interest.

- **Corporate control:** Contracting in and outsourcing are inevitable consequences of governments

committing to digitisation, because they rarely have the capacity to do the work themselves. The power relationship between the state and private corporations is turned on its head, as governments become captive of the tech industry. If the e-commerce rules say the government can't require a corporation providing the service from offshore to have a local presence in the country, it forfeits even more control. Faced with unaffordable costs of new services and upgrades, threatened or actual exit by the foreign providers, or technology or performance failure, governments have no capacity to step back in and resume control even if the rules let them.

- **Data:** Control of data is the key to everything digital. Governments rely on contractors to design, operate and process personal data from public and social services, and store it on servers. Often the data is stored 'in the cloud', which means the servers are located in one or more unspecified places, although they are usually controlled from the US. If the government agency has not been very specific in the contract about its data, it may have no control over what happens to it or even rights to access it for research or planning purposes. Once that data is out of government hands and held offshore there is no guarantee that protections and obligations under national law will apply or be enforceable. The e-commerce trade rule will prevent them requiring the data to be held locally, rather than offshore. While that rule excludes data held or processed by or for a government, there are many loopholes, such as national or service-specific data bases that non-government services providers also use.



- **Digital technology and source codes:** The source codes and algorithms that drive the government's internal systems, or public services more generally, are a black hole. But they are not abstract technicalities. Humans who create them have inbuilt biases and design them for specific purposes, usually to maximise commercial gains. Algorithms that are designed to learn from examples will replicate the bias in those examples. The e-commerce rules say the owner can't be required to disclose the code or algorithm in most circumstances, even assuming a government agency has the technical expertise to analyse the software. In most agreements that ban extends to inquiries conducted by a government agency like a human rights body, competition authority, privacy commission or even the Auditor General. Even where biases are detected, it can be difficult and costly to ensure they are changed as the supplier has total control over the software. There is an exception for 'critical infrastructure', but that is not defined.

- **Public infrastructure:** State-owned operators commonly contract tech companies to supply and operate the sophisticated and highly automated systems that operate public energy, transport and telecom infrastructure. Where public private partnerships are involved, their IT arm may be built into the special legal entity that is created for a particular project, with limited liablity or sub-contracted, including to an offshore operator. Indeed, the entire spectrum of operations - from smart grids, emergency systems and predictive maintenance to delivery, smart metering, and billing and payment systems – may be controlled externally, possibly from outside the country. What happens if the state has privatised control and has no human capacity to operate its essential services infrastructure in a crisis like a natural disaster, political sabotage, technology failure, cyber-ransom or civil war, or if the contractor fails financially or to perform its legal obligations? The e-commerce rules say governments can't require a legal presence in the country or presence to take a particular legal form.

  While the e-commerce chapters have an exception for government procurement, this only for non-commercial contracts for goods or services that are used for internal government purposes. The chapter does apply to the procurement of any service that is on-sold directly or as part of another service (such as a utility, IT connection or toll road). These e-commerce obligations are independent of the separate government procurement chapter, so the procurement thresholds or entities that are excluded from that chapter don't apply to the e-commerce chapter.

  In parallel, a digitised public infrastructure depends on and generates mass data, which gives the private corporations that run it access to and control over sensitive information about a country's entire infrastructure. Aside from potential for misuse, there are risks of digital sabotage or malware. The e-commerce rules allow forced disclosure of source codes and algorithms relating to critical infrastructure, but that was deliberately not defined and leaves it unclear what it might cover. Even where that seems cleacut, such as electricity or telecommunications, a government would need to be proactive to obtain ther software, which may not happen until the risk has materialised, and would need the skills to analyse it.

- **Employment and public service:** The trend to contract work and casualisation extends beyond the IT sector to core public service jobs. Hollowing out and deskilling the public sector workforce creates an expensive, long-term dependency on profit-driven private contractors who can't be forced to locate

onshore. Whether they are tech giants or IT professionals, they lack institutional memory and a professional commitment and culture of public service. Within the public service itself, automation and AI are replacing some jobs and significantly changing others without the necessary support and retraining. Algorithms are increasingly being used to replace human assessments, for example of health and safety or vulnerability, which deprofessionalises the work and puts the public at risk; yet even the government may be unable to access them under e-commerce trade rules.

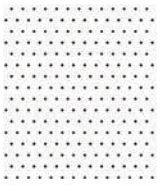
- **Working conditions:** The ideals of a professional public service are fundamentally challenged when employment decisions, such as hiring, promotion and firing, are delegated to indecipherable and unaccountable algorithms. Algorithms inform the psychometric testing and predictive analytics that decide who is hired, fired, or promoted, with the ability to screen out union members or non-subservient workers, and hide intrinsic gender, race or religious bias. Surveillance of workers' personal habits and behaviour, on the job performance and productivity, and out of work activities intrudes on personal space, increases stress and opens the way to harassment and discrimination.

- **Industrial relations and unionisation:** Structural shifts in public sector employment, including further privatisation and fragmentation, erode union membership and strength. The diffused structure of a highly contractualised digital economy makes unionisation much more difficult, and collective bargaining almost impossible. Who is the employer? How do you bargain with offshore firms? Who is the employment contract with and how is it enforceable? Who is held liable for breaches of collective contracts or labour laws and how?

- **Social wellbeing:** When governments pursue digital strategies in the name of inclusion that assume away the digital divide, they widen social inequality and marginalised communities are further excluded and disenfranchised. Because e-commerce trade rules are designed by and for Big Tech, those who suffer as a consequence are treated as invisible and irrelevant. The corporations can refuse to disclose the technologies they control, even when that is necessary to prove inbuilt and systemic racism and gender bias, anti-union discrimination, and violations of other fundamental human rights.

- **Public finance:** A long-standing moratorium on customs duties under e-commerce trade rules, the export of public funds to contractors located offshore, and falling revenue from tax avoidance by foreign digital firms comes at a time of growing demands on government services and support. Government spending is diverted to new technologies that rarely run to budget and need constant upgrading. These become budget priorities because the systems will fail without more investment and governments seek to avoid the political embarrassment of walking away. If the response is yet more austerity elsewhere, the public sector becomes trapped in a vicious circle of cuts to public service provision and staffing and increased reliance on technology.

These broad challenges will serve as the reference point for a more in-depth consideration of how the digital trade or e-commerce rules impact on two specific areas of public services in the Asia Pacific region. The case studies are not intended as a comprehensive account of the issues but aim to provide relevant examples of the impact of the e-commerce trade rules.



2.

Big Tech's 'Digital Trade' Demands

The use of the term 'trade' today can be very misleading. Only a very small part of today's international 'free trade' agreements is about old-fashioned commodity trade. As instruments of neoliberal globalisation, they are designed for, and often by, transnational corporations and financialised capital. The goal is to shrink the size and power of the state, expand the size and scope of profit-driven markets, and increase the global power of transnational corporations. As new sources of profit and expansion emerge, so the trade rules expand. Since the 1990s the agreements have targeted government laws and policies on services, including finance and telecommunications, government procurement, intellectual property and technological knowhow. Over the past decade, as the digital revolution gained momentum, there has been a new focus on electronic commerce or digital trade. As the subject matter expands, so do the restrictions on governments' right to regulate.

At their most basic, these 'trade' rules put handcuffs on what central, and sometimes local, governments can do in their laws, policies and practices behind the border. The core rules require governments to minimise or remove restrictions on foreign commercial interests, targeting rules that directly or indirectly restrict their activities and profits or that give preferences and protections to the local economy. When dealing with services, these restrictions apply whether the service is being supplied from outside the country, such as by the Internet, or by a local

branch of subsidiary. Increasingly, the agreements also dictate how government should go about making new regulation to ensure that foreign states and transnational corporations can intervene in the process.

Governments are required to prioritise commercial considerations over other their public policy responsibilities for development, social wellbeing, sustainability and climate change. Because international trade treaties are enforceable by foreign states and sometimes by foreign corporations they also take precedence over states' other international obligations, such as International Labour Organization conventions or United Nations' human rights instruments.

These agreements are designed to be forever. Once the government signs on, it is very hard to alter its obligations even if its negotiators misunderstood what they were agreeing to or it has damanging consequences they could not have foreseen. For legal, political and economic reasons, they are even harder to exit. The Trump administration's actions to quit the TPPA, force a revision of the North American Free Trade Agreement, and sabotage the World Trade Organization show it is possible for a powerful country to do so on its own terms, but only where it is able to withstand any retaliation and, in the US case, so it can exercise even more arbitrary power. The chaos surrounding Brexit shows how hard it is hard even for rich countries to unwind their deep integration.

BIG TECH'S DEMANDS AND THE DIGITAL 2 DOZEN PRINCIPLES

The easiest way to understand the new 'trade' rules on e-commerce or digital trade is to look at what the Big Tech lobby was asking for and why – because that is basically what is in the rules. Before looking at the details, it is important to recognise their significance to the US economy and politics. In 2019 the top four global companies by market capitalisation were Microsoft, Apple, Amazon and Google[3]. In 2018 Google was the highest corporate spender on lobbying the US Congress[4].

US law effectively insulates the tech companies from government intervention. As regulators wake up to the risks, Big Tech wants the guaranteed right to regulate itself or choose when and how it submits to external regulation - and not just in the US.

For more than a decade, various tech industry groups lobbied intensively for international 'trade' rules that would protect them from regulation on a global scale. In 2014 the Office of the US Trade Representative (USTR) published the 'The Digital 2 Dozen' (D2D) principles to guide future trade policy and negotiations. The D2D basically codified the industry's demands[5]. The electronic commerce chapter of the Trans-Pacific Partnership Agreement (TPPA) was the first to adopt them[6]. The US negotiator who signed off on the chapter, Robert Holleyman, had spent 23 years as the President and Chief Executive of the US Business Software Alliance. The USTR described the result as 'the most ambitious and visionary Internet trade agreement ever attempted'[7].

The TPPA has since become the template for free trade negotiations on electronic commerce. The US insisted on even greater protections for Big Tech in Digital Trade chapter of the United States Canada Mexico Agreement, adopted in December 2019. The US's determination to write the global rules for the digital domain is not simply to advance its corporate interests; it is also driven by the tech rivalry that is centre stage in its trade war with China.

The D2D principles that are most significant for public services are set out below, followed by a summary of the rule that was adopted in the TPPA. You will see how the interests of the tech companies are all framed in positive terms, and any policies or regulations that interfere with those interests use negative language like 'barriers', 'protectionism', 'discrimination' or 'forced localisation'. That's the benefit of

including them a trade agreement - corporate interests are guaranteed to take priority. The corporations also love the secrecy, which allows them to influence the negotiations and keeps everyone else in the dark.

- **"Promoting a free and open Internet".** On its face, this suggests an unrestricted Internet where you can choose your provider, don't have to pay for using it and no-one interferes with what you see or say. But people are becoming aware that more is going on behind the scenes. The Internet is not just a de-humanised technology that operates in a neutral space. People's user-experience is shaped by invisible decisions about what data is mined, where it stored and how it is used, and the the design of the source codes, algorithms and protocols that determine the results of an on-line search or a job application. Those decisions are made by human beings who work directly or indirectly for profit-driven corporations. While Big Tech controls how the 'free and open' Internet operates, it wants to be free from regulation or at most subject to voluntary codes. In another play on the word 'free', the price you pay for not paying money for the Internet is your data, which is much more valuable to the tech firms than the cost of supplying the service – although they can of course still charge for their services, especially once they have captured their clientele.

Article 14.10 says the parties 'recognise the benefits of consumers ... having the ability to access and use services and apps of their choice available on the Internet'. But 'recognising the benefits' doesn't impose any obligation on the governments or tech companies to make sure people can do so. Even then, access and choice are subject to 'reasonable network management' and a party's 'applicable laws, policies and regulations'.

- **"Prohibiting digital customs duties".** Most developing country governments still tax imported products at the border through tariffs or customs duties. That brings in revenue to fund the government and public services. Higher priced imports also provide some protection for local businesses and employers. Back in 1996 World Trade Organization (WTO) members agreed to a temporary ban on customs duties for electronic transmissions. That ban has been rolled over every two years at the WTO. Big Tech, digital exporting countries, and developed countries with low or no tariffs, want it made permanent.

  Electronic transmissions are not defined. According to the D2D, the ban on customs duties applies to all digital products, such as e-books, Netflix movies or 3D-printed designs. Developing countries like Indonesia insist that it applies only to the transmission itself, not the content. That difference really matters, because the amount of goods that are affected by the all-encompassing D2D definition is huge and growing every year. The revenue impacts will be enormous, especially for developing countries[8], at the same time as their governments face increasing demands to support local communities, workers and businesses that are negatively affected by digital disruption. The ban also removes an alternative that governments could otherwise use to tax technology companies that avoid conventional company tax.

Article 14:3 says there shall be 'no customs duties imposed on electronic transmission, including content transmitted electronically' between countries that are party to the agreement. Governments can still impose internal taxes, fees and charges, but only those the agreement otherwise allows. That means the tax must

not treat the foreign electronic content differently from the local equivalent.

- **"Securing basic non-discrimination principles".** Discrimination always sounds bad and competing on equal terms sounds fair. In practice, non-discrimination means ensuring that GAFA or Samsung and Fujitsu can out-compete local enterprises, including those in developing countries that are just beginning to develop strategies for digital industrialisation. The kinds of 'discrimination' that Big Tech wants to prohibit are special restrictions that apply only to them or preferences for local start-ups, such as relief from certain regulations so it's easier for them to compete, or supports like breaks for businesses that are embedded in communities that provide local jobs, pay taxes in the country, and use culturally appropriate content.

Article 14.4 says governments can't give preferences to local digital products just because they contain local content or were made locally. However, that doesn't apply to subsidies or grants. It also doesn't apply to broadcasting.

- **"Enabling cross-border data flows".** This is the D2D that matters most to Big Tech. Data is the raw material for the digital domain. Personalised data can be traced to an individual. Capturing, storing and selling this kind of data is invaluable for employers, insurers and other risk assessors, education and health providers, financial lenders and, of course, government agencies for both positive and coercive purposes. Personalised data also allows specific targeting of individuals based on their search history, preferences, spending patterns, friend groups, as well as their demographics of age, race, class, employment, location etc.

While data that is traceable to a person is important, huge data sets that reveals patterns and trends, and 'meta-data' that structures and manages mass data and gives a higher level of data about data, are ultimately more important and more valuable. The more data there is, the more accurate the analysis that informs the algorithms that generate profiling, targeting and predictions, and machine-learning or artificial intelligence (AI), such as online computer support, targeting advertising, Apple's Siri or Amazon's Alexia.

Data expands dynamically, giving first movers with an established web presence and captive user base an in-built advantage. Users generate data voluntarily, but usually unknowingly, through web searches, cookies and apps, using the GPS or wearing fit-bits. That data multiplies exponentially with every connection to networks - your Facebook friends, a like or a share. Pre-eminent search engines and social media platforms can entrench their dominance and make it almost impossible for late entrants to compete (and if they look threatening, they take them over). Predictably, Big Tech want a guaranteed and unfettered right to collect data and store, transfer, process, use, sell and exploit it anywhere in the world, or to prohibit when they describe as 'forced localisation' of data in the source country. First and most important, they want to transfer and store data in their place of choice. That is partly for efficiency, so they can process bulk data without having to duplicate facilities and personnel - but as importantly so they can choose destinations that have the most favourable laws. That usually means the US, which does not regulate the Internet and has weak consumer and privacy laws. Tax

havens are now becoming data havens too. Prohibiting 'forced data localisation' therefore makes it very difficult for governments to improve their regulation of the Internet.

Where governments insist that they need access to data for public policy reasons, Big Tech say that must be for a 'legitimate' public policy reason (are monitoring employers' labour practices such a reason?), and only what is necessary to carry out that purpose – for example, through a voluntary arrangement to make data that is held offshore available on request (what can the government do if access is urgent and/or an offshore firm doesn't comply?).

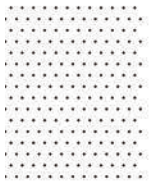
Article 14.11 says countries must allow data, including personal information, to be transferred out of the country electronically for the conduct of a business to which the agreement applies. There is an exception where a policy or law aims to achieve a 'legitimate public policy objective', which is not defined and can be contested. Even then, the law or policy can't involve 'unjustifiable discrimination' and the government has use the most light-handed approach reasonably available to achieve its policy goal, which Big Tech will always say means a voluntary arrangement or another form of self-regulation. 'Data held or processed by or on behalf of a government' is excluded. But it is not clear how that is to be defined; for example, would a national health data base that is not compiled by the government, or formally collected for a government purpose, be excluded?

- **"Preventing localization barriers".** Big Tech also wants to prevent other 'forced localisaton' requirements that they describe as 'barriers' to digital trade, such as the obligation to use servers located in the countries where they operate. Again, they say that is for efficiency and the cost of replicating sophisticated servers in each country. But it also ensures they can continue basing most of their servers, including 'cloud servers', in the largely unregulated US or other locations of choice. Further, developing countries have little incentive to invest in their own infrastructure if they can't require the big players to use it, perpetuating their dependence on large foreign providers.

Another localisation 'barrier' is a requirement that companies supplying services from outside the country have a local presence within the country. If they don't have a presence they can circumvent local legislation and taxes on their company profits much more easily. It can be almost impossible to get those companies to court, to require production of information in a dispute, or to enforce penalties, for example, for unauthorised data sharing, tax dodging, negligent health services or breaching labour or discrimination laws.

Articles 14.13 says a government can't require a business covered by the agreement 'to use or locate computing facilities' (meaning 'computer servers and storage devices to store or process data for commercial use') in the country as a condition of doing business there. As with data, there is an exception where a policy or law aims to achieve a 'legitimate public policy objective',. Again, it can't involve 'unjustifiable discrimination' and must be the least restrictive way to achieve the policy goal. Articles 10.6 says a government can't require a business that supplies a service from across the border to have a legal presence inside the country, and Article 10.5(b) says if it is present in the country it can't be required to take a particular legal form.

- **"Prohibiting forced technology transfers".** Technology-poor countries, especially in the global South, need access to technology if they are to develop and become self-sufficient. Transferring technology is a common condition for approving



a foreign investment. Tech companies describe that as theft of their intellectual property and want any such requirements banned. They also want to prevent governments from requiring them to employ local people in positions that would given them access to 'proprietary' or company knowledge; in other words, they can block local workers from positions where they would learn high-tech skills and limit them to low-value low-tech jobs.

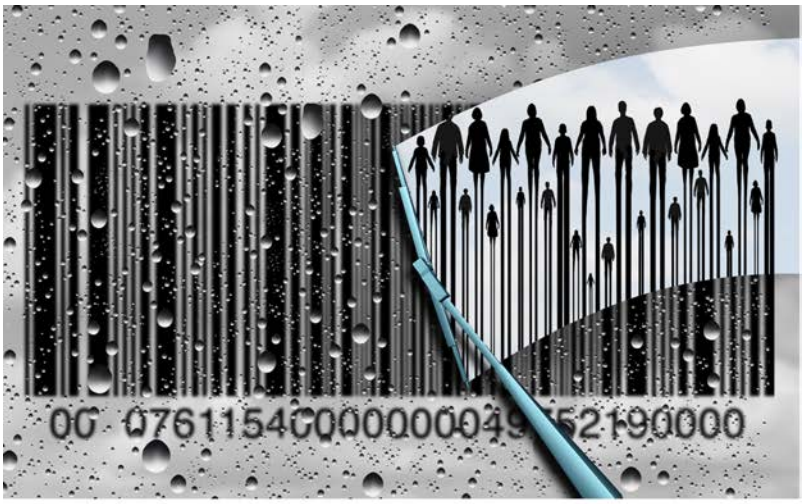
Article 9.10.4 says a foreign investor can't be required to 'transfer a particular technology, a production process or other proprietary knowledge' to someone in the country as a condition of setting up or running an investment there, or to buy, use or give preference to locally made technology. They also can't be required to employ or train workers if that would require transfer of technological or proprietary knowledge to those workers.

- **"Protecting critical source code and algorithms."** Source code instructs computers about what to do and is integral to the design of software. Code is written by humans in a language that humans can read and transformed into binary code that the computer can read. Algorithms are sequences of rules or actions (rather like a cooking recipe that uses ingredients as inputs, follows a number of steps and produces an output). They are put in effect by the source code in order, for example, to process mass data into patterns and predictions or to make choices between applicants for jobs, social welfare, medical treatment or bank loans. The tech companies want to keep the instructions they give to computers secret, even from governments. This would make it almost impossible, for example, to expose racial or gender biases in psychometric testing or sentencing, profiling of workers as anti-union or immigrants as terrorists, wage theft through flawed measures of productivity, or anti-competitive or fraudulent practices, or to check the vulnerability of smart products, such as smart meters, to hacking or malware.

Article 14.17 says a foreign owner of source code that is used for mass-market software or products can't be required to transfer or disclose it to anyone in another party, including the government. There is an exclusion for 'software used for critical infrastructure', which is not defined. It also remains possible to require disclosure of software as part of a commercially negotiated contract, which means both parties will have to agree the terms. (Recent agreements have a more blanket ban on requiring disclosure of source codes, and the US-Mexico-Canada agreement explicitly prohibits requirements to disclosure algorithms as well.)

- **"Delivering enforceable consumer protections".** This is not as positive as it sounds. Big Tech knows that trust is important and they can't be seen to reject the need for consumer protections. But they can ensure that those protections are minimal and difficult to enforce. The consumer protection laws in their main home-base, the US, are weak, complicated and decentralised and rely heavily on enforcement through the US courts. Even where countries have strong consumer laws it can be incredibly difficult to protect the rights of consumers on-line and provide effective remedies, especially when the supplier is offshore: the consumer or the government agency needs to identify who is legally responsible, where they are located, what laws apply, and then work out how to pursue them in either the local or the offshore courts and enforce any outcome.

Article 14.7 says countries must have a 'law to protect consumers from fraudulent or deceptive activities that cause harm', but there is no minimal standard that the law

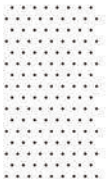


© Shutterstock 2020

must meet. Article 14.8 requires the same for the protection of personal information or privacy (which Big Tech in the US treats as a subset of consumer protection). Again, there is no minimum standard and a footnote says this can include voluntary arrangements that are enforceable. Article 14.14 says governments must adopt measures on spam, but the options would allow most existing practices to continue.

- **"Building an adaptable framework for digital trade".** New technologies, apps, smart products and services are being developed all the time. Facial recognition software, unmanned drones, cross-border robotic surgery and 3D printing were the subject of sci-fi movies 20 years ago. What will their equivalents be in another 20 or 30 years' time? Big Tech want to ensure that rules adopted today will apply to any digital products and services developed in the future. In other words, governments should blindly commit to rules that surrender their right to regulate any unknown and unknowable digital products and services for the indefinite future, with very few exceptions.

This also ensures that economic activity mediated by digital technologies, whether at the level of national digital development or individual innovation, will remain captive of those who control the 'digital eco-system' of data, search engines, platforms, market-places, logistics and payment systems.



Articles 9.11, 10.7 and 11.10 require governments to draw up and negotiate two lists to protect their services and investments from some of the rules. Annex 1 lists the existing laws on services or investment the country wants to maintain, which would otherwise breach core services and investment rules; any new liberalisation (making those laws more market or corporate friendly) would be automatically locked in. Annex 2 lists the activities, laws or categories of services or investment for which the country wants to keep open its ability to regulate in the future, such as aspects of health policy or broadcasting. These lists have to be agreed on by the other parties and are almost impossible to change. (There is no equivalent list to exclude measures from the e-commerce rules, except where they overlap.)

- **"Securing robust market access commitments in investment and cross-border services".** 'Trade in services' agreements guarantee foreign firms that provide services can invest in countries or sell their services across the border, mainly by the Internet, with minimal restrictions. The WTO's General Agreement on Trade in Services (GATS) dates back to 1995 and services chapters are now standard in FTAs. Governments used to say which services would be covered by the rules and list any limitations on their exposure. Even that was problematic, because privatisation brought more public and social services under private, often foreign, control. Once a service was committed it would be almost impossible for a government to take back control even if circumstances had changed, there was a new social need, or a government was elected with a mandate to restore public services.

  Big Tech wants governments to go further and list any activities or policies and laws they want to protect from the services and investment rules, which they would have to negotiate with the other parties. Whatever is not listed, including unforeseen new technologies and services, will automatically be covered by the rules. From its perspective, the industry sees this 'negative list' approach as future-proofing the agreements. Critics see it as profoundly anti-democratic. Governments don't have a crystal ball. They will make mistakes and new needs or challenges will arise. Super-neoliberal governments might deliberately make very few reservations, knowing future governments cannot reverse what they have done.

Chapters 9, 10 and 11: The entire chapters on cross-border services, financial services and investment are designed to restrict government's ability to decide how to regulate all those digital activities.

- **"Promoting cooperation on cybersecurity".** Breaches of cybersecurity that wreak havoc at a national level, or cause distress and harm to individuals, are becoming all too familiar: hacking into computers to steal welfare data or tax records, installing malware to sabotage transport infrastructure, seeking a ransom to remove a virus from computers across a government or even across countries, stealing sensitive data and passwords from customer data bases. The culprits may be another state or private actors and come from anywhere in the world. While Big Tech demands lots of guarantees for themselves, they are only suggesting that governments should 'cooperate' on cybersecurity.

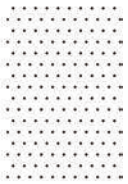
Article 14.16 says the parties 'recognise the importance' of building the capabilities of their cyber-security response teams and using 'existing collaboration mechanisms to cooperate' to identify and mitigate 'malicious intrusions' and malware. Again, this wording doesn't impose any obligations on governments and no constraints on Big Tech.

- **"Ensuring fair competition with state-owned enterprises (SOEs)".** Many developing countries use SOEs to provide public goods and deliver services. In some countries they are a vital part of the domestic economy, with many other businesses and workers dependent on them. Today, many SOEs are required to operate commercially and make a profit. But tech firms say even those SOEs still enjoy an advantage because of their government status. They claim it is unfair that they can't compete on a level playing field in those countries, or in third countries where they and the SOE both operate. The tech lobby wants full access to government procurement by SOEs and to ensure there are no special tax, regulatory or other benefits. Applied strictly, this would prevent governments from supporting local start-ups to reduce the country's dependency on big foreign firms and ensuring those corporations don't gain control of the national infrastructure and data. While Big Tech's main target is China's SOEs, these rules would have a major impact on all countries that have existing, or are creating new, state entities to develop their digital capacities and protect the national interest.

Chapter 17 is the first ever full chapter on SOEs in a free trade agreement. Is says SOEs can't prefer local firms when they buy or sell goods or services. SOEs also can't receive a commercial advantage (such as tax treatment, different regulations, or other benefits) if that adversely affects another party's business. When that rule involves services, it only applies to services the SOE supplies outside the country, but their domestic and cross-border activities are often inseparable.

- **"Promoting foreign tech company participation in national policy making".** Big Tech calls this 'transparency'. They don't mean ensuring the public can see what is happening in negotiations or in the commercial operations of tech firms themselves. They want a right to participate when countries they operate in are developing new policies, regulations and technical standards that affect them. In other words, so they can lobby, threaten to bring investment disputes, run public scare campaigns, and otherwise use their massive resources to stop or dilute proposed restrictions they don't like.

Article 26.2 says the government must provide full information about existing rules and practices, and 'to the extent possible' give foreign businesses prior notice of changes and the opportunity to comment. Article 13.22 has stricter obligations to allow input from telecom firms on proposed regulations that affect them. Article 25.5 'encourages' governments to use regulatory impact assessments that favour no or self-regulation. (This chapter was seriously diluted after it was leaked. The US-Canada-Mexico agreement has much stricter obligations to allow foreign companies to be involved in the policy-making process.)



3.

Digitised Healthcare

Quality health, education and welfare services are essential public goods. The first case study in this report looks at key issues arising from the digitisation of healthcare and the likely impacts of the e-commerce trade rules, using the South Korean government's digital health strategy as the main example.

PRIVATISATION OF PUBLIC HEALTH SERVICES

Digitisation promotes the privatisation of public health services in several ways:

- The familiar form of privatisation involves public health authorities contracting in or outsourcing the provision and management of technologies and data to private firms and consultants, because they lack the technological knowhow to run their own digital systems. Contractors for digital health services are rarely healthcare specialists and often adapt generic technologies and skills to the healthcare system.

- Public health services can become casualties of a government's broader strategy to build its digital economy if the health market is viewed simply as another growth opportunity for the profit-driven tech sector. The focus on commercial opportunities for existing corporations or start-ups can subordinate the social and human dimensions of health services to other priorities if appropriate protections are not put in place.

- In countries where public and private health facilities are not-for-profit, incorporating health into the general digital economic strategy can provide an entry point for privatisation of the health system per se. That can trigger important battles to protect the integrity of the country's non-profit health services.

- Health tourism is another revenue-raising enterprise where private, and increasingly public, healthcare providers offer overseas users a service they can't buy at home. 'Tourists' may be attracted by the low price, capitalising on cheap labour and operating costs, and/or by access to advanced services using new digital technologies. When governments buy into the digital health tourism model, the promotion of healthcare as a commercial business erodes the primacy of healthcare as a social service.

Challenging Korea's back door to privatisation[12]: Jeju Greenland International Healthcare Town was launched in 2008 to develop a medical complex combining (health) tourism, healthcare, and research and development of biomedical products in the island's special economic zone. In 2017 Greenland Group, a state-led Chinese conglomerate, built what was to be Korea's first for-profit private facility, mainly to cater for wealthy Chinese tourists. A majority of locals voted against the hospital in a referendum secured by opponents to the plan, including the Korea Health and Medical Workers' Union. Although a partial license was granted the license was revoked, prompting legal action from the Chinese developers.

Healthcare as a digital growth strategy: In 2017 South Korean President Moon Jae-In established a Presidential Committee to oversee The People-Centred Response Plan for the 4th Industrial Revolution to Promote Innovative Growth (Industry 4.0)[9]. He predicted economic gains of some US$560 billion; more than a fifth of that would come from the healthcare sector[10]. The vision was presented as a win-win: new technologies will enhance the health conditions and quality of life of individuals, expand welfare, reduce costs for patients, and promote economic growth. Yet the overriding goal was to grow the healthcare technology industry and increase the country's competitiveness. Technology, especially AI, would be integrated throughout the domestic health system – a system that is totally dominated by the private providers, but funded by the national insurance scheme. The South Korean finance ministry invested $3.2 billion dollars in the Industry 4.0 strategy in 2019 and proposed USD3.9 billion for 2020, about 8% of which would go to bio-health[11].

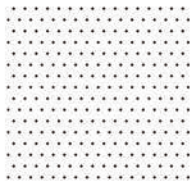
WHAT THE TRADE RULES SAY:

Trade in services and e-commerce rules create the conditions for privatisation, although they don't require it. Ideologically, health and digital services are treated as marketable commodities. The goal is to expand health markets nationally and internationally to the benefit of foreign firms.

The core trade in services rules require governments to remove barriers to foreign firms that provide digitised health services, whether as foreign investors or by remote delivery from offshore, and to allow a country's nationals to go overseas for health tourism. Governments often try to protect health services from the trade rules, but that's more difficult in recent agreements that require them to list what the rules don't cover. Public health services are only excluded from the rules if they are not commercial and they are provided by a monopoly public provider.

Where health services are part of a country's digital economic strategy, the fact they are health services may be incidental. Both the tech corporations and government are likely to see them as computer-related or even property development services, to which they have usually agreed to apply the trade rules, rather than as health services. Governments that are committed to this economic strategy are unlikely to invoke any health-related exceptions that might be available to justify protecting their health systems from privatisation.

CORPORATE CONTROL



Transnational corporations routinely design their corporate structures to minimise their regulatory obligations, compliance costs and tax and legal liability by basing themselves in countries that are most-corporate friendly. Digital technologies allow the providers of the health-care service, or those who own and operate the technology, to deliver services across the border, or centralise their global operations, such as R&D and data storage, processing and analysis. There are major legal and practical problems in protecting users' rights or ensuring insurance coverage if the healthcare or technology providers are located offshore and have a minimal or no presence locally.

A small number of transnational corporations dominate the health technology industry at national, regional and global levels. They have such market power, and scales of research and development and data that it is almost impossible for new entrants to compete, unless they are already big players in another sector. Many of these corporations are tech giants that have branched out into healthcare as a profitable growth sector. Governments' ever-deepening dependency on such firms transfers public power over crucial decisions to private corporations that are unaccountable to citizens, put profits before ethics, and have no commitment to people's health needs.

Sometimes the tech giants compete with each other for contracts in both public or private health care systems, but the big players are just as likely to enter into partnerships that pool their expertise and intensify their market power.

The lobbying power of Big Tech is ever-present at global and national levels to secure policies and laws that work for them and stop those they oppose, and to convince countries to use their services and products, even when they are under a cloud elsewhere.

Samsung in control: South Korea's Samsung Group dominates the healthcare sector. Samsung Medical Centre is one of the country's leading hospitals with services heavily funded by National Health Insurance reimbursement. Samsung Life Insurance is the largest in South Korea. Samsung SDS is the IT services arm that operates across 30 countries. In March 2019 the pharmaceutical unit Samsung BioLogics, a joint venture with US-based BioGen Inc, was accused of accounting fraud[13]. Samsung Bioepis was set up to manufacture bio-similar pharmaceuticals company, again with BioGen; after BioGen took control in late 2018 Bioepis no longer had to report on its licensing agreements and update shareholders on progress with clinical trials[14].

Samsung, Philips and Microsoft: Samsung ARTIK Smart IoT platform and Philips HealthSuite Digital Platform announced a partnership in March 2018 to provide inter-operability and link Samsung's 'ecosystem' to Philips cloud platform. The massive integrated data set would feed their 'enhanced health analytics'[15].
Another Samsung arm, Samsung Seoul Hospital, signed a Memorandum of Understanding with Microsoft Korea in 2017 to create a new AI-based precision health care system using Microsoft's cloud platform Azure, for application in clinical decisions on patient care and disease specific prediction models[16].

Letting Big Tech regulate itself: In a speech to the Korea Healthcare Congress 2018 a senior official from Google health subsidiary DeepMind Health called for the deregulation of all AI-based healthcare[17].

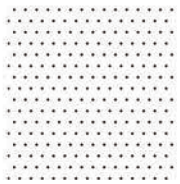
WHAT THE TRADE RULES SAY:

Trade in services rules say governments can't restrict foreign firms from supplying health services across the border or through investments in their country, and can't limit the number and size of a corporation's operations. Governments also can't give preferences to local firms or require them to use local content or hire local personnel for high-tech positions. Nor can they require a firm that supplies the service from outside the country to have a local presence in the country, or if there is one, that it takes a legal form that makes it more accountable under local laws.

Importantly, many governments have protected their health services from these rules, or limited their application when they adopted these agreements. But companies like Samsung and Microsoft say they are providing computer services, which lots more countries have committed to the rules.

The 'transparency' rules in these agreements are a lobbyists' charter, guaranteeing them a say over proposed new laws that might affect them.

DATA



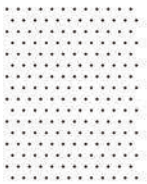
The tech corporations make big money from their contracts for health-related services. But the real gains for the health tech firms come from the massive pools of data that they generate and collect. They may use that data themselves to develop and enhance their own sophisticated algorithms and AI and/or sell the data to other tech firms. There are at least three ways they can profit from the data and deepen the dependence of the country's healthcare system on them:

- **operating the data systems** that link various health entities together across the entire healthcare system, from private primary care to public hospitals to health insurance to integrated national data bases. These systems generate massive data pools that are (usually) outside the control of the public health authorities, who become captive of the tech/data owners.

- **storing and using personal health-related data,** mainly in the 'cloud'. The rules and protections that apply to personal health data are crucially important, given the serious direct harm that use for an unauthorised purpose or a privacy breach can cause. On-sale of personal data is lucrative, for example to health insurers, employers or marketing agencies. Even when consent to collection and use of personal data is required, few users read the fine print or understand the implications. Where a country does have strong domestic protections, breaches may be difficult to detect and prove, and even harder to enforce if the data is held offshore and/or the service provider has no local presence.

Selling health data from apps :
A joint University of New South Wales and Harvard Medical School academic study showed 33 of 36 smartphone apps used for depression or to quit smoking sent data to outside organisations; 29 of them were to Google or Facebook. Very few of the apps had any privacy statement[28].

Don't trust Google with data:
The UK National Health System contracted a Google health subsidiary DeepMind Health to process patient records of UK citizens for several London hospitals, without seeking patient consent. The information included details of drug overdoses, abortions, and whether individuals were HIV positive. The UK's data protection watchdog found the Royal Free NHS Trust had no legal basis to share its medical records with DeepMind[29]. DeepMind continued contracting with the NHS, promising the data would never be connected to Google accounts or services, nor would machine learning or AI tools be used to analyze this information. In 2018 Google announced it was moving DeepMind into the main company in preparation for global expansion. It insisted that strict audit and access controls would remain. Now the data sits on Google Health's servers. Privacy experts described the transfer as a betrayal of patient's trust[30].



- **aggregating anonymised mass data,** such as data from medical records, diagnoses, prescriptions and medical trials is even more valuable to health tech firms than personalised data, because that is what drives the algorithms and AI on which the new technologies are based. Researchers also show that most individuals whose data is anonymised can be relatively easily re-identified[21].

DIGITISED HEALTHCARE

Mining mass health data: In 2017 96% of South Korean hospitals and clinics used Electronic Records Systems[22]. That system generates a massive pool of data for potential use. A study showed there was a lot of sharing within each organisation, but low levels of external links. That was expected to change under South Korea's Industry 4.0 strategy. The strategy includes a single health and medical big data platform, bringing together the National Health Insurance Service, the Health Insurance Review and Assessment Service, the National Institute of Health and the National Cancer Centre. A pilot 'Healthcare Big Data Showcase Project' will integrate and analyze health/medical/genetic data of 300 healthy people and cancer survivors, accumulate healthcare big data-using experiences, and utilize the data to develop standardized data from 2019 to 2021[23]. The new platform will be a data-bonanza for South Korea's chaebols that are deeply integrated into the national healthcare system.

WHAT THE TRADE RULES SAY:

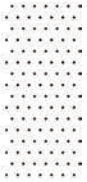
The e-commerce rules allow businesses to transfer data out of the country to wherever they want. An exception for 'legitimate public policy' reasons is limited to the least interference with the company's rights, which they are likely to say means a voluntary arrangement to make data available on request. Because governments can't require businesses that supply a service from outside the country to have a local presence, it may be practically impossible to monitor and enforce compliance with such voluntary arramgements or with local laws that govern the use of health data.

The e-commerce chapter clearly applies to private health firms. There is an exception for health information that is 'held or processed by or on behalf of the government'. It is unclear whether that extends to government supported projects, especially when private healthcare businesses and private health data are involved. The rules also exclude procurement of the IT system for the government's own use, provided there is no commercial use of the service. That would not cover systems that charge health providers or professionals for access, or where the service itself or something created with it is onsold to other users.

THE HEALTH TECHNOLOGY INFRASTRUCTURE (INCLUDING SOFTWARE)

There is a broad spectrum of healthcare activities that rely on digital technologies:

- offshoring the analysis of lab tests, bloods or x-rays, and the operation of digitised record systems;
- web-based management systems used for online bookings and to manage drug inventories, schedule interventions, and roster staff, including from private personnel firms;
- drones used to deliver meds and bloods, especially to remote locations;
- interactive consultations in real time, which expedite decisions on diagnosis and treatment;
- predictive diagnostics, monitoring and management through algorithms used to prioritise interventions and allocate resources;
- tele-health and interactive websites and apps that encourage self-diagnosis and self-management;
- smart technologies built into automated drug trolleys in hospitals and equipment for self-medicating or self-managing patients; and
- surgeons conducting AI-driven robotic surgery remotely, including across borders.



Many of these technologies offer efficiencies and can improve the quality of health services. Integrated health platforms and technology systems can also improve coherence. However, they create long-term dependency among health providers. Health providers are already finding that sunk costs lock them into a particular system or supplier that requires compatible hardware and software, and specially trained personnel, with regular upgrades. Seeking add-ons or adaptions from a different supplier is problematic as they usually need access to data, technological information and source codes. There is also no guarantees that the old and new systems will be compatible. Where there is system failure or a better technology becomes available, the entire system may need replacing at huge expense and serious disruption.

Many of these products are unregulated or lack rigorous certification requirements because they are so new. They rely on proprietory source codes and algorithms that are poorly understood by and inaccessible to outsiders, because they are treated as commercial secrets. That makes it almost impossible to evaluate their accuracy or safety, including their cybersecurity, or to prove liability for negligence or fault (even assuming health or other regulatory authorities have the necessary skills). Information about failures may only become available through a whistle-blower or access to internal documents.

Software failure: IBM Watson is a question-answering computer system to assist clinicians make decisions. Watson for Oncology was initially hailed as the solution for cancer treatment. Internal documents from mid-2017 show the system was heavily criticised by users, who said it frequently provided bad, and sometimes dangerous, recommendations for treating cancer patients. That did not stop IBM from promoting it to hospitals and doctors around the world[24]. Nine South Korean hospitals contracted to use the expensive equipment[25], but scepticism about the system, and differences in patient profiles, limited its uptake. Samsung Seoul Hospital has partnered with Microsoft to develop its own system.

WHAT THE TRADE RULES SAY:

The source codes and algorithms that drive digital health technologies are mainly owned by the Big Tech firms. They want to keep them secret. The rules say governments can't require them to disclose them.

Some agreements would exclude the health system if it was defined as 'essential infrastructure', which the agreements don't define. Others don't have that exception. Some would allow regulatory authorities access to investigate compliance, others only to enforce an outcome of an investigation, and others ignore the issue altogether.

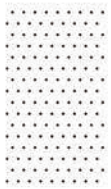
The firms that dominate the sector also can't be required to invest through joint ventures or transfer of technology so local firms can develop the technological capacity. Where local start-ups do exist, they can't benefit from preferential treatment.

EMPLOYMENT, WORKPLACE AND UNIONS

As the Digitalisation report for PSI notes, there can be positive outcomes in the workplace where technology enhances work experience and relieves health workers of menial or unpleasant tasks. But even where there are benefits, other impacts can outweigh them. Hospitals and other facilities often fail to invest in training to use new technologies or to offer retraining instead of redundancies. Displacement by technology and/or contract workers, often from offshore, results in job losses, de-skilling, and stress. Over-reliance on technology can endanger lives when there is a technology or system failure and there are no manual back-up systems and trained staff to step back in. There are also serious ethical and professional concerns when technologies remove the human element from clinical judgements and algorithms replace context-based assessments by health professionals of people's health needs.

Selective retraining: The South Korean government's Industry 4.0 plan promises to nurture experts who can collect and manage big data, using the AI platform and provide education for employees at pharmaceutical companies to help them carry out studies using the AI platform. There is no equivalent emphasis on employment of health professionals.

When there is no local presence, there are no jobs and no training or development. Local pay, conditions and job security are undermined by the use of cheaper offshore providers, such as call centres or diagnostics. Competition among such countries fosters a race to the bottom on a regional and global scale. Local qualification and registration requirements are almost impossible to enforce and depend on what requirements and enforcement of them apply offshore. It may be impossible even to identify which country the service is provided from. Where foreign firms operate from inside the country they usually import their own management and senior professionals rather than employing locals.



Digitisation in the workplace fundamentally changes the public employment relationship and carries risks when it use is invisible and unaccountable. Algorithms can be used to screen suitably compliant applicants for jobs and promotion against undisclosed profiles, and micro-manage and constantly reorganise daily routines. Workplace surveillance and tracking that monitors productivity can be used to justify wage theft on spurious criteria and inform threatened or actual disciplinary action. Data collected on workers' health, personal qalities, qualifications, family and friendship networks, and out of work activities may be used to feed automated

Union resistance: The Korea Health and Medical Workers' Union (KHMU) is a staunch opponent of privatisation and mobilised with civil society groups in the successful campaign against the Jeju Greenland Hospital[28]. The union fears the loss of traditional medical jobs as new tech-based work is developed, with no discussions yet of training and upskilling of the workforce. Already those working with digital technology are reporting increased workloads and added stress. KHMU has been promoting meaningful participation of labour in social dialogues and decision making with creation of a tripartite body on health and medical issues.

decisions and predictions that affect their work and private lives, and be onsold to other users, such as health insurers or credit agencies.

Public health systems are often among the most highly unionised, especially public hospitals. The private healthcare workforce is not. Nor are contracters working within or outside the country. De-unionisation and de-professionalisation go hand in hand, with consequential impacts on the quality of service and patient welfare. As collective action becomes harder to organise and less effective, unions have to strategise across sites, sectors and countries to consolidate their position. Transnationals that operate from one or more hubs can neutralise industrial disputes by shifting service supply from one place to another.

WHAT THE TRADE RULES SAY:

There are no protections for workers or labour standards, only for corporations.

Local labour laws don't apply to offshore firms. There may be a mutual recognition arrangement for offshore qualifications, but health unions have no right to participate in those decisions.

Foreign firms can't be required to employ local people in higher skilled jobs if they would gain access to knowledge the business wants to protect. Algorithms remain secret. Control of data remains with the employer and data protections are weak.

SOCIAL WELL-BEING

New technologies may improve access to health services for remote areas - if those communities have inter-connectivity. Where there is a serious digital divide, greater reliance on technologies in place of face-to-face services and local facilities is set to deepen that divide.

Likewise, existing gaps between high-tech for-profit health care and the public system and its users will widen. In theory, public health services should improve when wealthy local and international users migrate to private facilities, because there is less demand. In reality, public health providers are left to perform essential services for poorer communities who have less leverage to demand quality health care or latest technologies. At the same time, national health digitisation strategies may require the public health system to buy expensive technology it can't afford at the expense of other services and pool its data to the benefit of the Big Tech companies.

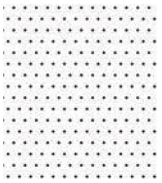
The shift from public to private and personal to digital also changes the nature of healthcare services. The culture, values and priorities of tech corporations give priority to efficiency, rationing and profit, not to public service, health ethics, and social obligations. The human right to health and the state's human rights obligations to indigenous people, minorities and women and gender sensitivity are at risk.

Algorithms can't replicate cultural, gender, age and ethnic sensitivities, human judgment and compassion. Because source codes and algorithms are written by humans, their culture, gender, class or religion will inform the assumptions embedded in their programmes. Algorithms that are designed to learn from examples depend on the quality of those examples. Biases will be impossible to detect without access to the source code or algorithm (or even with access, unless there are expert analysts available). The public system and health professionals are not perfect, but they can be held to account if and when rights violations occur.

When even industry leaders recognise there is a lack of evidence to support using AI in the health system, there are very real dangers of bias for those who depend on the system, and no-one is accountable, there is an urgent need to restore the public good and social wellbeing to health policy decisions.

Harvard Medicine: "AI is subject to the principle of 'garbage in, garbage out,' … If the input has a systemic bias, the model will learn from that as well as from actual signals. … Overlooking bias in medical AI invites serious consequences. Recommendations based on biased models or inadvertent misapplications of a model could result in increases in illness, injury, and death in certain patient populations. … The US has no requirement to test for bias in AI and no standard for determining what bias is[27]."

Lloyd McCann, Head of digital health, Healthcare Holdings, New Zealand, 'The inconvenient truth about AI in health': "There is no sign that the use of AI, or machine learning algorithms is going to slow down, the opposite is in fact going to happen, it's likely to speed up. … And yet there is a relative paucity of evidence to support its use in healthcare. … How do we manage bias in algorithm development? There is a narrative that almost tries to blame the algorithm for that bias, the blame doesn't sit with the algorithm, the blame sits with us and the datasets we've used to develop those algorithms because our data sets aren't necessarily representative of the populations we're trying to serve[28]."



WHAT TRADE RULES SAY:

Tech firms have no corporate responsibility obligations.

Source codes, and recently algorithms, can be kept secret. The level of privacy and consumer protections are left up to each country - but which country's rules will apply depends on where the service is supplied from and/or where the data is held.

There is a general exception for health measures, but that requires a government to use the most light-handed option available to achieve its health policy goal, rather than putting health objectives first, and is subject to other restrictions. Human rights, gender, indigenous rights and culture don't rate a mention in the exception.

PUBLIC REVENUE

DIGITISED HEALTHCARE

In theory, the free and open Internet encourages easy of entry and competition that drives prices down. In reality, the anti-competitive dominance of the tech giants, especially over data, is locked in. Yet these mega-corporations structure their ownership and operations to pay almost no tax in any country where they operate. The health tech sector is no exception. Because most health tech firms are foreign and have complex tax-based structures, an increasing share of public health funding goes out of the public system and often out of the country, with no corresponding tax income from the corporate beneficiaries or the workforce. Mega-national firms often operate the same.

Costs associated with digitisation are absorbing a growing share of countries' public health budgets. The small number of transnational corporations that dominate the health technology sector set the price and continue to aggressively market their products, even when the evidence doesn't support their claims.

The high cost of digital technologies has to be funded by increased health expenditure or diverting funds from other budget priorities, reductions in services and staffing, closing facilities, offshoring activities like analysing test results or x-rays to low-cost countries, and/or raising revenue through user charges or market-activities like medical tourism. The investment also often requires maximum utilisation. That creates incentives for unnecessary procedures, especially where private sector operators can recoup the costs from a public health insurance system. Sale of health data offers another lucrative source of revenue.

WHAT THE TRADE RULES SAY:

There are no protections in these agreements against oligopolies of big corporations collectively inflating prices to maximise profits. Because companies can't be required to have a presence in the country where they operate, public and private health funding goes directly out of the country, and chances of effective enforcement of tax laws are even more remote. Even where they are present, they can organise it so the revenue goes offshore and the limited legal form of their local entity means they have no tax liability. Governments can't cap the amount of their income they call royalty payments and send to their offshore tax havens. The tax exceptions in trade agreements are incredibly complicated and largely unworkable.

In 2018 the South Korean government announced plans to impose new taxes on global tech companies like Google and Apple, which are notorious tax avoiders and benefit from the tax law that says only companies with a fixed place of business in the country have to pay tax[29]. South Korea's own chaebols, which are central to the country's digital health streatgy, also engage in tax planning to minimise their tax liability. In 2019 Samsung was convicted for intellectual-property related tax evasion[30]. The Samsung family have their own history of tax evasion, including a high-profile conviction of the patriarch and company chair in 2009 and new charges laid in 2018[31].

Robotic surgery: Da Vinci Surgical systems is a robot that a surgeon controls from a consol. It promises less damage and a faster recovery than older forms of surgery, but after 15 years research found little improvement on older forms of laparoscopic (minimally-invasive) surgery for a lot higher cost to both hospitals and patients[32]. That has not deterred the US-based owner Intuitive Surgical from promoting it globally. In late 2017 the company opened an innovation and training centre in South Korea, where Da Vinci was already being used in 51 hospitals[33].

Central and local governments are run by elected politicians and professional public servants. That is their job. Harnessing digital technology to help them serve their people better - more effectively, inclusively, democratically and efficiently - seems unquestionably good. It can be, if governments take a measured approach to utilise technologies for the public good, with openness and accountability in procurement, building local public and private sector capacity and skills, and ensuring robust protections for citizens' rights are in place.

'Smart cities' promise to deliver those benefits as a win-win for everyone. Yet the 'smart city' slogan has become an ideological extension of a neoliberal agenda that has dominated public policy for decades, and it is expanding in the Asia Pacific region. Examples from India, South Korea, Indonesia and Singapore show how digital technologies are being harnessed to serve the neoliberal priorities of efficiency, cost-savings and market growth, especially at local government levels. In the process, governments are transferring more of their public responsibilities to unaccountable mega-corporations that control the technology and the data used to run the cities. The e-commerce trade rules help make that happen and may make it very hard to change direction.

PUSHING THE PRIVATISATION AGENDA

THE WORLD BANK'S SALE PITCH :

"When we think about Smart Cities we usually go in one of two directions.
1. A technology-intensive city, with sensors everywhere and highly efficient public services, thanks to information that is gathered in real time by thousands of interconnected devices … All buildings are 'intelligent', with smart meters and energy savings systems, and transport is painless.
2. A city that cultivates a better relationship between citizens and governments - leveraged by available technology. …
We believe that both approaches are not mutually exclusive, and that they can be adopted by cities in developing countries to improve the delivery of public services. In essence, we propose a smart city development framework[34]."

This latest mode of privatisation has familiar origins. For several decades, the World Bank and Asian Development Bank (ADB) imposed disastrous structural adjustment policies on Asian and Pacific countries, including mass privatisation of public assets and services. Now they are pushing a 'smart cities development framework' with the promise that information technology, fuelled by mass data, will deliver a win-win for capital, governments and citizens. The same flawed assumption is in play: that social wellbeing, development and democracy are best served by governments transferring power and resources to the private sector, this time the Big Tech transnational corporations.

The China-led Asian Infrastructure Invest-ment Bank (AIIB) is another 'smart cities' funder, supporting technologies for intelligent traffic and transit, e-road pricing, smart outdoor lighting, environmental monitoring, and smart grid and metering. Like the World Bank and Asian Development Bank, its projects are financed by government and private funds or through public-private partnerships (PPPs)[35].

In the Asia Pacific, Singapore, India and South Korea have led the way.

Singapore's futuristic 'Smart Nation transformation' operates by 'leveraging sensors, the Internet of Things and data analytics to tackle a diverse range of problems, from traffic congestion to healthcare'.

Singapore aggressively exports its model to the region. Singapore, the US Trade and Development Agency, France, Japan, and Dubai are all active partners in India's Smart Cities Mission to transform 100 cities across the country over five years[37], the region's most ambitious and controversial project to date.

Whether the Smart City is a greenfield or a retrofit, it will also involve the privatisation of publicly owned land, as well as water, sanitation and other services. Along the Delhi Mumbai Corridor, for example, state governments provided 130 acres of land for 37 companies in 2018, including 100 acres to South Korean conglomerate Hyosung[40].

South Korea's failing Songdo project provides a warning to other countries seeking to jump on the smart city bandwagon.

WHAT THE TRADE RULES SAY:

Most smart city projects operate through public procurement. Recent e-commerce and services chapters exclude government procurement, but define it very narrowly. The service, including IT, must be used only for the government's in-house operations and it can't be charged for directly, or as part of a service the is charged for. Contracts for services like street lighting and traffic control, which are not directly charged for, should therefore be safe from the trade rules. But contracts for transportation, public housing, utilities or online data retrieval, and for inputs into those services such as IT, will be subject to the rules when users of the services have to pay. The integration of services and data in 'smart cities' and the consolidatation of data it impossible to separate services that are subject to or exempt from the rules. That becomes especially important when governments have made commitments, or listed reservations, to the rules based on specific services sectors.

South Korea's white elephant: Songdo was built from scratch on reclaimed land as part of the Incheon Free Economic Zone. Incheon U-City Corporation began as a PPP between Incheon Metropolitan City, KT (Korea Telecom) and US company Cisco; by 2016 the city held less than third of the shares[41]. Songdo is hardly a success story. It was to be completed by 2017, but was less than half-built by 2018 at a cost of $40 billion[42]. The city was described as 'overdue, overpriced and underpopulated' with 'Chernobyl-like emptiness', and a 'ghost-town' with few residents or big businesses moving there. One rescue remedy was to create an American Town within Songdo, with the aim of attracting attract Korean-US residents to return home[43].

Singapore smartest city in the world: The inaugural IMD Smart Cities Index - based on a poll of just 120 residents and co-sponsored by the Singapore University of Technology and Design - declared Singapore the 'smartest city in the world' in October 2019[38].

Modi's urban renewal agenda: In June 2015 India's Prime Minister Narendra Modi launched the Smart Cities Mission (SCM), a multi-billion flagship urban renewal programme with the aim to transform 100 cities across the country[39]. The promise: citizen-friendly, inclusive, and sustainable cities that were cost-effective, transparent and accountable[39]. The central government announced a two-stage nationwide competition/challenge process. All states and union territories, except West Bengal, participated by nominating at least one city. As of February 2019, 100 cities had been chosen based on four rounds of competition, which cover 5151 projects at a cost US$ 30 billion (2.05 lakh crores).

CORPORATE CONTROL

Smart cities are big business. US corporations Cisco and IBM have specialised in promoting them since the mid-2000s. South Korea's Songdo was one of Cisco's first projects. Familiar names like IBM, Microsoft and Oracle are also on board. Consultancies like KPMG and Deloitte offer self-serving advice. McKinsey Global Institute produced a report in 2010 entitled 'India's Urban Awakening' and subsequently hyped the big data revolution as the pathway to productivity and economic growth for India's urban development[44].

Influential transnationals formed the global Smart Cities Council. Its 'lead partners' are AT&T, Oracle, Aviva, the Centre for Innovative Technology and WeGo (described as an association of 170+ 'city and other local governments, smart tech solutions providers and national and regional institutions'[47]). The Council provides an online platform (an 'Activator') to help cities plan and deploy 'smart' projects and runs a Smart Cities Readiness Network to to expand its support base and link supporters in the public and private sectors. The Council has national lobby groups. There is a branch in India. Its website for Australia and New Zealand says its director has 'spent more than 20 years influencing infrastructure and urban regeneration projects across the world[48].'

'Smart cities' usually operate through Public-Private Partnerships (PPPs) that sub-contract to private corporations, or by government procurement contracts for private-private collaboration among technology, telecom, construction, software and hardware firms.

Consultants get Java on board: In 2019 the Governor of Indonesia's West Java, a province of almost 50 million people, decided it should become a Digital (and 'Smart') Province, following the consultancy report The Digital Komodo Dragon: How Indonesia can capture digital trade opportunity at home and abroad commissioned by the corporate-sponsored Hinrich Foundation[45]. West Java's ICT Department pitched 19 PPP projects to corporate stakeholders at a 2019 event in Singapore[46].

India's arms-length PPPs: For India's 'smart city' projects, central and local government are shareholders in Special Purpose Vehicles (SPVs) who then enter into procurement contracts with private tech and other companies. Each of India's Smart Cities Mission projects involves a distinct SPV, which is a separate legal entity and limited company created at city-level. The State/Union Territory and the Urban Local Body jointly have a 50:50 equity shareholding. The SPVs convert the Smart City Proposals into projects, hire project management consultants and staff, and enter into partnerships with corporations (e.g. for software/digital applications in public services)[50].

The corporate lobbying network: The Smart Cities Readiness Network describes itself "as a global knowledge exchange for public sector employees. It offers a weekly newsletter, in-person workshops, discounts to smart city conferences, and a way to find and connect with cities working on similar projects. Membership in the Readiness Network is free of charge to public sector practitioners who have demonstrated a commitment to smart city progress, such as: If your city has hosted a Readiness Workshop, participated in the Readiness Hub at Smart Cities Week … If your city is using Activator … Public sector employees who have significant smart city responsibilities may join individually[49]. "

The SPVs have limited capital and assets, and hence limited potential liability. They may be exempt from some regulatory obligations or from complying with local laws altogether. Rules on foreign direct investment are usually relaxed for them – although digital technologies enable some foreign firms to operate without any local presence. The city administration may have one or more directors on the board, whether or not it is a shareholder in the SPV. Those directors are usually public officials, not elected local government representatives, which further distances them from electoral accountability.

"As Bhopal is recast as a Smart City, its poor have a question: The Bhopal Smart City Development Corporation has state and municipal officers on its board but no elected representative. It is housed in a new luxurious building next to the dingier offices of the Bhopal Municipal Corporation. It is well-funded and empowered to generate revenues by outsourcing services and initiating partnerships with private players. Its budget is separate from the municipal corporation's. There is an advisory body that includes elected representatives, but its recommendations are not binding.[9]"

WHAT THE TRADE RULES SAY:

Where the government procurement exception doesn't apply, there are serious restrictions on how governments can regulate the private service suppliers involved in the SPVs or other contracts, unless they have reserved the right to do so in their schedules. For example, they can't restrict the number or size of foreign firms from a country that is party to the agreement, or even their rights to access inputs, including owning or leasing land. They can't require a foreign firm supplying the service to have a presence in the country or, if they are present, to use a particular legal form that would make them more liable, including a joint venture. Nor can they require a majority of local directors on boards, or any local senior managers, or the employment of local workers if they might gain proprietary knowledge.

The right of foreign firms to know in advance and comment on new regulations that might negatively affect their interests is as important, given their lobbying power and risks of corporate capture of central and local government decision-makers.

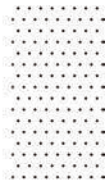
DATA

World Bank, World Development Report 2016: Smart Cities.
"By collecting large amounts of data and then translating these data into insights, cities are able to boost the efficiency and responsiveness of their operations. Data help cities better match the supply of public services with real-time needs and uncover emerging problems before they turn into crises. Smart city technologies make this possible in several ways. Automated optimization translates data from cameras, sensors, and anonymized cell phone records into intelligence to, for example, help optimize traffic flows in real time. Predictive analytics uses such data to track and predict everything from rainfall to crime hot spots to possible landslide areas. Evidence-based decision making and planning can continuously monitor milestones and targets to ensure cities can quickly take corrective actions as needed to achieve their goals[53]."

Governments, including city administrations, have a unique power of legal coercion to collect data. People have to provide personal information to access essential services, such as water and sanitation, or for public services like libraries, and sometimes just to live their everyday lives. Cities are responsible for the information that is entrusted to them. If they involve third parties in the collection, storage, use of that data, they have ethical and often legal obligations to maintain that trust. That becomes practically and legally difficult with smart cities that devolve or contract out those functions to private firms, who may hold the data offshore or operate from outside the country.

Cities can and should regulate where and how data can be collected. With 'smart cities' that is not just by surveillance cameras in streets, buildings, carparks, bars and public spaces, and from PPP toll roads, library cards, sports teams and soup kitchens – in South Korea's Songdo it is sourced from inside people's homes. New Zealand's state housing agency plans to do the same[52]. That personal information can be highly sensitive. The risks from privacy breaches and abuse by state agencies and private corporations are obvious. But there are also major issues with the anonymised mass data that people and agencies produce on a city-wide basis and that is harnessed without consent. That data generates the valuable software, algorithms and AI that drive 'smart cities' and enable the corporations to expand the programme globally. As with healthcare, what assumptions and biases are fed into these technologies can positively or harmfully affect people's lives.

The boundaries between public and private data are blurred. Non-government entities who deliver devolved or outsourced services for the 'smart city', from social welfare and child care to property registries and parking enforcement, will feed data into and access shared data bases as part of their work. It is no longer purely government data. More fundamentally, as the smart city runs on mass data, so it generates more data in a perpetual process. In Songdo, for example, home heating, security, parking and deliveries are all controlled by a central 'brain' that uses data collected across public and private spaces to constantly refine its analytics[54]. It actively promotes the use of public data for R&D to be used for commercialisation and private profit. That gives the autocratic Singapore government and its collaborators economic and political power.



It is not clear who owns and controls publicly-sourced data and how can it be used. Even if governments are partners in a 'smart city' PPP, they may not control the data - and if they do have a say in its use, their practices may be as commercial, invisible, unaccountable and anti-democratic as the transnationals. Central and local governments may also end up spending public money to buy data that privately collected from the public domain for its public planning purposes.

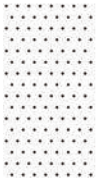
WHAT THE TRADE RULES SAY:

Because smart cities by definition generate masses of personal data, the right of tech firms to send and use it wherever they want in the world leaves the residents of smart cities with minimal protection. The trade rules allow governments to restrict information that is held or processed by or on behalf of a government – but it is not clear how far that applies to the hybrid public-private arrangements in 'smart cities'. If governments can't require data to be held onshore or on local servers, they have to fall back on the public policy exception. They not want to do that when the whole object of smart cities is to have data-driven decsions and the main legal vehicle involves SPVs with private, usually foreign firms. The exception also requires the least burdensome restriction on the company's activities, and the tech firms are bound to argue that voluntary arrangements to make data available to the government is a less burdensome alternative. Governments can impose privacy rules, but they are often behind what is required. There are no effective protections for the mass data that is the gold mine for the tech firms involves in smart city projects.

'Virtual Singapore' allows 'scientists and urban planners to conduct experiments and run simulations through a data-rich, 3D model of Singapore at the touch of a button'. Singapore's 'start-up ecosystem' the Launchpad, established in 2011, is a collaboration between NUS (National University of Singapore) Enterprise, the incubator of the telecommunication company Singtel and the Media Development Authority of Singapore. As of 2018 it involved 14 'accelerators', 23 'incubators', 439 'start-ups' and 15 'investors/venture capitalists'[44].

Public buy-back of public data: "In New Zealand, Qrious, a [private telco]-owned software company, has been providing customers' location data to local government bodies for the last three years. Now, it's experiencing an uptick in demand from central government agencies. Those agencies are also exploring other sources of location data, such as Google and GPS manufacturer TomTom, to help inform decisions and planning. The Ministry of Business, Innovation and Employment has recently moved from using only official government statistics to incorporating private data[45]."

THE TECHNOLOGY INFRASTRUCTURE



Songdo on-line: "The smart city project of Songdo is largely divided into six sectors including transport, crime prevention, disaster prevention, environment and citizen interaction, to provide smart applications. Other services relating to Home, Store, Learning, Health, Money and Car are also actively being developed. Songdo has the most advanced Integrated Operations Command Center in Korea and their integrated smart city services are provided, not only for Songdo, but for nearby cities too[56]."

"SMART CITIES"

Local governments supply many, and in some cities most, of life's essential services: water, sanitation, electricity and transport infrastructure, affordable housing, a sustainable environment, safety and security, health and education[57]. In 'smart cities' that usually includes IT connectivity and digitisation. All local authority services, including citizens' engagement with government, are digitised and integrated through a single 'brain'. Operating that brain is usually contracted to Big Tech multinationals, giving them the ability to switch an entire city on or off.

Public administration, especially at local authority level, rarely has the expertise to set the specifications and select the best tender for a technology procurement contract, let alone oversee the performance and compliance of successful bidders. They are a captive of their consultants and the corporations who run the digitised infrastructure and essential services, which may sub-contract and operate the systems from offshore. Where problems arise, the city administration has to face the problems of contract termination, finding another provider and system compatibility. Capture also makes them dependent on external advice and solutions to technology and software failures, hacking and malware, and even deliberate sabotage, which pose new, potentially catastrophic risks as everything becomes digitised.

Legal liability for infrastructure failure can be limited by a lack of transparency, the terms of the contracts and the structure of SPVs and their lack of assets. This is even more problematic when the service provider is located offshore. Corporate capture of governments can chill them from taking legal action and result in expensive compromises.

WHAT THE TRADE RULES SAY:

As noted above, it is unlikely that the exception for government procurement in the e-commerce chapter applies to all, or even most, of the smart city activities. Where it doesn't apply, the government can't require the foreign firm providing the service to have a presence in the country, unless the government reserved the right to do so. If it has set up in the country, the government can't require it to transfer technology, hire and train locals in its technology, or use local content, such as locally produced software, all of which would build local capacity. Instead, foreign firms would have the right to import their own skilled personnel or hire foreign consultants, unless the government's schedule says otherwise. There are no guaranteed cyber-security protections.

International Electrotechnical Commission cyber-warning:
"Critical infrastructure facilities, whether they are power plants, national railway and local underground systems or other forms of public transport, are increasingly being targeted. Cyber attacks could cut off the supply of electricity to hospitals, homes, schools and factories. We rely so heavily on the efficient supply of electricity that its loss would also carry heavy implications for other vital services.
A number of incidents in recent years demonstrates not only that the threat is tangible, but also that on more than one occasions we have escaped incurring nightmare consequences by the skin of your teeth[88]."

ALGORITHMS AND SOURCE CODES

'Smart cities' operate through source code and algorithms, AI and the Internet of Things, which are built on mass data that is harvested locally and elsewhere. Bad data generates bad results – garbage in, garbage out. If the data collected is skewed by race, gender, age, the software and algorithms based on it will be too, even if those who write them are unbiased. However, they are not unbiased. The Big Tech workforce is predominantly white and male, and their assumptions inform the software and algorithms they write[60]. Those biases are especially important because 'smart cities' are using biometric programmes provided by Big Tech for everything from policing and social security to privacy protections on their personal data.

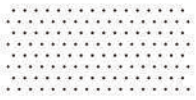
The technology that governments rely on is commonly developed offshore. Singapore's biometric programme, for example, is being developed with UK company GDS, whose own facial recognition scheme Verify has been fraught with problems.

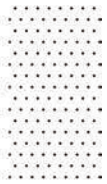
Biometrics used by local authorities have been linked to fundamental human rights abuses, especially race and gender profiling.

There is a real risk that similar techniques may be used to identify and suppress unionists and communities that resist the Smart City projects. India's recent court ruling creates a worrying precedent that these biometric profiling may be considered both constitutional and consistent with national privacy laws.

Singapore surveillance: In 2003 the City state of Singapore introduced the National Digital Identity portal SingPass for all Singaporeans over 15 years to prove their identity online and in person across public and private sectors[61]. In October 2018 Singapore released the Singpass Mobile app which allows citizens to conduct secure digital government transactions using biometrics (fingerprint, facial recognition) for authentication rather than passwords, including from offshore. Trial biometric systems were rolled out at sea and airports and lampposts. The app can be downloaded from Google Play or App Store[62] and be used to check on pension funds, apply for public housing[63]. Singapore is working on a centralise biometric scheme, beginning with facial recognition, to use for a number of services. Singapore also still has the communist era Internal Security Act on its books which allows detention without trial for posing an actual or potential threat to security.

"SMART CITIES"





Singapore's UK partner: After long delays, Verify was eventually introduced in 2016. By 2018 its development had cost £154 million. A UK Audit Office report in 2019 described Verify as "an example of many of the failings in major programmes that we often see, including optimism bias and failure to set clear objectives[64]."

Lessons from the UK: "A study published in July 2019 showed a London policing trial that relied on facial recognition software produced by Japanese supplier NEC to spot suspects had an 80% failure rate, meaning harassment. The police defended its continued use[65]."

India's mass data profiling deemed constitutional: The Indian government's Aadhaar biometic identity programme, using biometric profiling, stores data centrally in the Unique Identification Authority of India (UIDAI) and has become the largest data base in the world. It aims to cover the entire Indian population and act as the basis for all interaction between the government and its citizens, as well as access to public services. Since 2016, registration has been compulsory for access to most welfare and social services, and there are plans to connect it to individual health data in the future. Enrolment into the programme is outsourced to private operators. In 2018, despite mass protests, the Indian Supreme Court declared the programme was compatible with the Indian constitution and the country's data protection legislation, because providing a digital identity gave dignity to the marginalised that was more important than privacy[66].

WHAT THE TRADE RULES SAY:

Residents of smart cities have no rights under these agreements, they have to rely on government action to protect them. Governments can't require the disclosure of source codes (and recently, of algorithms) except software for critical infrastructure. It's possible to argue that the technologies and related software in a 'smart city' are so deeply integrated that the government the whole project qualifies as critical infrastructure, so the government can demand disclosure. That would be hard to argue if the reason for seeking disclosure was to identify breaches of anti-discrimination or employment laws. Assuming the parties hadn't agreed to software disclosure in their commercial contract and the infra-structure exception wasn't available, the government would have to rely on the general exception for public morals or public order to justify making the owner hand over the source code. The government would have to prove it was justified and necessary to so, and it has no reasonable alternative that would impact less on the owner's rights.

EMPLOYMENT, WORKPLACE AND UNION

Trade union leader Jammu Anand from Nagpur Municipal Corporation Employees: Already under the JNURM [Jawaharl Nehur National Urban Renewal Mission] program, the pre-conditions for the financial support to the local body was to freeze recruitment for sanctioned posts under local bodies. Instead, the needed additional workforce was brought in through contractors and sub-contractors, and thus denied the service conditions defined for regular public servants. The nature of contracts is complex making it harder for an employee to prove his relation with an employer. Sub-contractors change regularly, and the principal employer, the local government body, is too many steps removed.

For many years, the systematic outsourcing and contractualisation of work at regional and city levels has eroded the size and stability of the workforce and working conditions, including job security, wages and conditions of employment, and morale. PPPs and the SPVs they operate through apply private sector employment conditions that are inferior to the public sector. Short-term contracts and constant pressure to cut costs mean frequent layoffs, workloads intensify and vacancies are not filled. If the SPV fails, it may lack the capital to pay unpaid wages or redundancies.

Foreign tech corporations generally bring their own senior managers and technicians, especially for jobs that involve proprietary knowledge. Countries that have invested in educating a tech-skilled workforce, or public sector workers who retrain, have no guarantee they can access quality jobs. If governments take the 'smart city' path and then experience policy failure, price-gouging or simply change their priorities, they will no longer have an adequately skilled public service workforce that can step back in.

An unstable, fluid and privatised workforce is hard to unionise, let alone for the workers to bargain collectively from a position of strength. Unions have little or no role in the contracting process or setting its terms, such as guarantees that existing workers will continue to be employed on the same terms in a transfer of undertakings.

Contract workers have little job security. Precarious employment makes union membership risky and union advocates an easy target.

Complex contractual relationships under PPPs and SPVs, with many layers of subcontractors, makes it very difficult for public agencies or unions to monitor or enforce employment terms in the master contract, such as a minimum wage rate for all workers in the project. When the main contractor is offshore, it becomes almost impossible. The local government that made the contract has no legal responsibility either.

On a positive note, union activism against smart cities continues the long tradition of public sector workers and unions mobilising to protect the public good, their unions and their jobs.

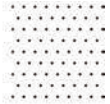
More lessons from Nagpur: Workers face serious difficulties to access labour courts and labour conciliation systems in the event of a dispute, be it for unpaid wages, discrimination or victimisation. Establishing the employer-employee relation leads to a lengthy and laborious process. Further, labour cases often rely on the disclosure of company documents. For instance, in a current case of difference of wages between the contractual arrangement and the wage actually paid to workers, the labour commissioner had to intervene so that the company disclose the proof of wages actually paid.

Jammu Anand on their experience in Nagpur … Another implication is the difficulty to join and create trade unions. Workers are afraid to lose their jobs and companies use the precarious conditions to resort to union busting even before a union is formalised.

WHAT THE TRADE RULES SAY:

If the ILO had a convention on digital workers the trade agreements wouldn't recognise it. There are no effective labour protections and no recognition of, let alone power, to trade unions – only to foreign governments and corporations. Even if strong labour chapters did exist, they wouldn't reduce the real risks to workers that come from the rules themselves. Government can't require a firm that is supplying a digital service from across the border to have a local presence, and consequently can't require it to employ local people. A contract may specify a minimum wage to prevent local competitors being undercut, but that may be impossible to monitor, let alone to enforce. The government can't require a foreign firm to employ and train IT or other staff at a high level, where they would gain proprietary knowledge, as a condition of the firm establishing itself in the country. Where there is a local presence, that may be through a shell company or delinked from the revenue earning operations, making it impossible to enforce local laws or judgements against the private contractors (which is already a problem with companies). Anti-union practices, wage theft, discrimination and privacy breaches can all be shielded by rules that protect the tech companies from having to disclose their software.

Nagpur Municipal Corporation Employees: "Now, our focus is on reaching out to contractual workers who are providing public services. A new relationship has emerged, public services have been provided by the contractual workers and not anymore by public servants. This is the change that has come into existence.
This is a gigantic challenge before the unions. First is they must come into terms with the changes taking place. Second is to understand the whole concept of public services; that outsourcing of public services means basically giving up the concept of being a public servant. People should understand that public services managed by private entities only deteriorates the quality of public services and leads to higher taxes. These are the new things happening for the unions to cope up with, reorganize themselves and organize with civil society. It is a big challenge. As a union we have taken up this challenge[47]."



SOCIAL WELL-BEING

Bhopal, Madhya Pradesh:
"Currently, the most visible feature of this enterprise are bulldozers. Eleven schools, one hospital, 3,000 quarters for government employees, hundreds of shops and two slum clusters have been razed or await demolition by the Bhopal Smart City Development Corporation, a company established for turning Bhopal smart. Unlike other cities that are 'retrofitting' existing colonies to make them smart, Bhopal is developing a 'smart area' from scratch. North and South Tatya Tope Nagar wasn't the first choice, however. The Bhopal Municipal Corporation's original proposal was to redevelop Shivaji Nagar and Tulsi Nagar. But their residents protested. With retired doctors, journalists and bureaucrats in their ranks, their voices were heard. The axe then fell on North and South TT Nagar[60]."

'Smart cities' prioritise efficiency and profit. They are the antithesis of empowerment in terms of social equity and governance.

The iconic image of skyscrapers, state-of-the-art airports, retail and trade centres, and massive uncongested highways has no place for the poor, informal street vendors, or slum dwellers. India's Prime Minister Modi's Smart Cities Mission promised adequate and assured water, electricity and sanitation, efficient public transport, affordable housing, especially for the poor. In reality, the fast track approval and implementation of 'smart city' plans that bypass laws or ease up regulations have left ordinary citizens, especially the poor and marginalized out in the cold and (literally) disconnected from their 'smart, citizen-centred' city. Gentrified enclaves are celebrated, while neglected areas are to be erased.

Nominally, the city's elected politicians and administrators remain in charge of and accountable for core functions and decisions. But effective control over information and the operation of essential services - from environment, planning and zoning to education, libraries and cultural facilities, to roads, transportation and public spaces – vests in the corporations that construct and operate the technology ecosystem. Those who hold public office can hide behind the commercial confidentiality of procurement contracts and sub-contracts. Crucial contractual terms, such as guarantees of land, rules on the location, ownership and use of data, or responsibility for systems failure, are screened from public scrutiny and political accountability.

Each community has different profiles and needs. Most 'smart cities' treat services as generic commercial products, using off-the-shelf programmes that fail to capture the unique characteristics of a particular sector or city. Algorithms have no capacity for human empathy or to understand social complexities. Interactions are depersonalised - it can be literally impossible to talk to a human person to solve a problem. Workers in the informal economy are forcibly displaced from their communities, especially by capital and land-intensive 'smart city' projects, which presents a challenge to traditional employment based trade unions.

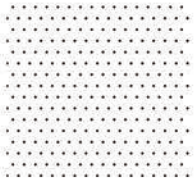
Likewise, 'good governance' through e-Governance and citizen participation replaces face to face democratic engagement. Participation assumes IT connectivity and digital literacy. Vulnerable communities who are further repressed and disenfranchised have to respond the only ways they can.

WHAT THE TRADE RULES SAY:

There are no protections in these agreements for communities and no requirements for governments to be accountable to their citizens. Occasionally, the rules encourage transnational corporations to adopt voluntary social responsibility codes. That bias no surprise. Trade agreements have always been designed by powerful states to serve their corporate interests. Digital trade rules are the latest, and arguably the most dangerous, version. Governments that embrace 'smart cities' transfer their public responsibilities to super-powerful corporations who are protected from accountability and liability in the name of e-commerce or digital trade.

ILO Report June 2019: The trade union movement in general must remain committed to promoting workers' rights in the informal economy, ensuring the improvement of their working conditions and enabling them to play a decisive role in the economic and social development process of their respective countries[69].

Resistance in Dholera: "Violently imposed on landscapes and populations who were presented as 'lacking' in development and therefore ideal for a 'makeover', smart city Dholera thus produced a protracted struggle for land rights and social justice even before it was built"[70].



PUBLIC REVENUE

'Smart cities' provide high returns for private players at low risk. Central and state governments provide the funds directly from their budgets or reserves, through the bond or equity markets, or by seeking out private, usually foreign investors.

Lessons from India: Modi[71] government allocated Rs 7,060 crore (a little over $1.1 billion) in its maiden union budget to kickstart the smart cities project. It had high expectations of attracting investors in a rapidly growing market, with industry forecasts ranging from US$39.5 billion to as much as US$2.1 trillion by 2020[72]. However, the investment rate has been slow, and cities are unable to mobilize the needed funds from the private sector. Indeed, as of February 2019, 53% of the projects under SCM are still in the tendering stage and only 39% of the projects are either completed or being implemented[73].

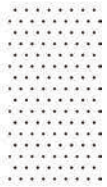
It is standard for PPP contracts to include a government guarantee of a minimum return to the SPV for a number of years. Although these obligations may not appear as debt on the public sector balance sheet, the government guarantee provides a secure income stream to private and foreign corporations from the public purse and gives them priority over many other forms of public debt. Governments become locked in to the smart city model while in effect taking on long term debt in the same way as old structural adjustment programmes.

Public money may go straight out of the country as foreign investors take their profits offshore. Profit shifting to tax havens through bogus royalties for IT systems is standard practice. Meanwhile, the SPV structure shields the private players from liability. They may just walk away, leaving the central and/or local government with a failed project that requires massive new investment to rescue – and potentially, a significant additional long-term debt.

As India's grand Mission shows, there is no guarantee that investors will come even on such terms.

When private investors fail to materialise, they pull out, or governments change, resources will have to be diverted from other public purposes and the price of privatised services increased, or the state and taxpayers will be left with an expensive unfinished project.

Local communities, workers and taxpayers who have no say in the policy decisions pay the financial, as well as the social and political price. 'Smart cities' can become a perpetual drag on government resources that should be used elsewhere. If they fail to achieve their goals, or even become financially self-sufficient, there is a political as well as fiscal cost for a government to walk away. Faced with this challenge, communities can and have fought back.



WHAT THE TRADE RULES SAY:

The rules facilitate profit shifting by tech corporations, who must be allowed to export their earnings and profits offshore. A favourite tax avoidance strategy is to transfer most of their revenue as royalties to offshore companies. The trade rules prevent governments from capping royalty payments as a condition of a foreign investment. As with digital healthcare, tax exceptions in these agreements are incredibly complicated and Big Tech companies are experts at gaming the rules.

Even where the foreign firm has a legal presence it can't be required to adopt a particular legal form; for example, it can set up shell company to avoid liability, including for failed projects. But where governments try to take back control they risk legal disputes from foreign investors demanding compensation for breach of contract. They may also be sued by the investor under the investment chapter of the 'trade' agreement for lost expenditure and future profits (something not addressed in this report, but nevertheless a very real accompanying threat). Faced with such risks, governments may simply to back off. They are left carrying the cost one way or another.

World Bank abandons Amaravati, Andhra Pradesh "Amaravati was promised as a dream come true – a utopia. However, the city, which was being developed as the new capital of Andhra Pradesh, now stares at a bleak future — after the pullout of major investors, as well as the lack of political will due to change of government in the state. … The World Bank explained that the government of India had withdrawn its request to the World Bank for financing the proposed Amaravati Sustainable Infrastructure and Institutional Development Project[74]."

Communities fight back: The World Bank intended to invest US$300 million, AIIB US$200 million and $215 million from the Andra Pradesh government for the Amaravati capital city project. In July 2019 the World Bank withdrew financing after massive local resistance against the project, citing its adverse environmental, social and economic impacts[75].

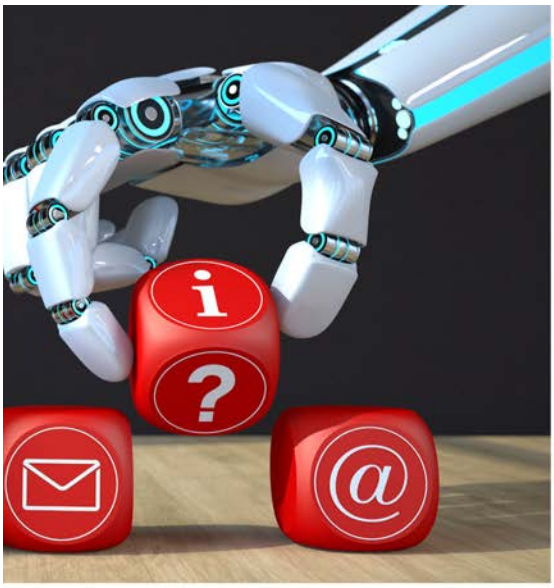
5. Recommendations

Based on the outcomes of this study, the following recommendations are made for PSI in the Asia Pacific region.

This study examines a small number sectors in some detail from the perspective of the implications for quality public services, decent work and the public interest, and identifies a range of concerns. Considering the lack of detailed studies on the implications of e-commerce negotiations in other public services sectors and countries in the region, PSI needs to demand that governments conduct extensive and broad-based research, in addition to research that PSI undertakes itself.

PSI should demand, at the least, a moratorium on e-commerce negotiations until that research is done and an informed debate and risk assessments have been conducted at national, regional and international levels, to determine whether such agreements should proceed and if they do, with what essential safeguards.

To advocate effectively on these issues PSI needs to investigate what is happening with digitisation of public services in different countries. This should look particularly at who owns and controls data, what can be done with it and what disclosure and accountability laws exist or are planned, with similar inquiries for source codes and algorithms that are becoming integrated into the public sphere . Models for public control of data created and collected through public services and public service workers should be explored.



PSI should work with other concerned unions, civil society groups and think tanks to map countries that have or are currently negotiating e-commerce and related texts and establish a comparative data base between different agreements. The main reference used in this study is the TPPA and it can serve as a barometer to assess other agreements.

A further, more specific investigation should be commissioned into the implications of the e-commerce texts from the perspective of industrial relations' legislation and workers' rights, such as legislation on discrimination at the work place, jurisdiction of courts and enforcement where employers are situated in another country, workplace health and safety, and surveillance and privacy of workers data. Legislation of key countries in the region can be used to reflect the diversity of existing law. The report should also highlight areas that require attention in legislation and collective bargaining.

Finally, PSI should coordinate education and activist campaigns against e-commerce negotiations in FTAs involving countries in the Asia Pacific region and in the WTO. Recognising the realities of digital transformation it should also identify other international fora for developing a progressive regime of regulation of cross border transactions in the digital economy, including the ILO, and develop strategies to develop and progress such alternatives.

REFERENCES

1. ITUC, The Future of Work, ITUC Report, 18 October 2017, https://www.ituc-csi.org/the-future-of-work-ituc-report; TUAC, Digitalisation and the Digital Economy. Trade union key messages, OECD, February 2017, https://www.ituc-csi.org/IMG/pdf/1703t_tu_key_recommendations_digitalisation.pdf.
2. Eckhard Voss and Raquel Rego, Digitalisation and Public Services. A labour perspective, Public Services International/Friedrich Ebert Stuftung, October 2019, https://publicservices.international/resources/news/psi-launches-new-report-on-digitalisation-and-public-services-from-a-labour-angle?id=10297&lang=en.
3. PwC, Global top 100 companies my market capitalisation, July 2019, https://www.pwc.com/gx/en/audit-services/publications/assets/global-top-100-companies-2019.pdf
4. 'Google Spent More than $21 Million Lobbying an Increasingly Tech-Nervous Washington in 2018, Fortune, 22 January 2019
5. https://ustr.gov/about-us/policy-offices/press-office/reports-and-publications/2016/digital-2-dozen
6. The US withdrew from the TPPA before it came into force and it was revised by the remaining 11 parties as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership that came into force in December 2018. The rules relating to electronic commerce were unchanged.
7. USTR (2016), The Trans-Pacific Partnership, https://ustr.gov/sites/default/files/TPP-Ensuring-a-Free-and-Open-Internet-Fact-Sheet.pdf
8. Rashmi Banga, Growing Trade in Electronic Transmissions. Implications for the South, UNCTAD Research Paper No. 29, UNCTAD/SER.RP/2019/1, February 2019.
9. https://www.4th-ir.go.kr/home/en
10. http://www.koreaherald.com/view.php?ud=20181210000652
11. https://about.bnef.com/blog/south-koreas-budget-puts-3-9-billion-industry-4-0/
12. https://www.koreatimes.co.kr/www/nation/2018/12/119_259913.html;
13. http://www.koreaherald.com/view.php?ud=20190314000779
14. http://www.koreaherald.com/view.php?ud=20190405000694
15. https://www.healthcareglobal.com/technology/philips-and-samsung-partner-develop-integrated-healthcare-services
16. https://www.healthcareglobal.com/technology/microsoft-korea-and-samsung-seoul-hospital-sign-new-mou
17. http://www.koreabiomed.com/news/articleView.html?idxno=3016
18. 'UK data regulator says DeepMind's initial deal with NHS broke Privacy law', TechCrunch, 4 July 2017, https://techcrunch.com/2017/07/03/uk-data-regulator-says-deepminds-initial-deal-with-the-nhs-broke-privacy-law
19. https://www.theguardian.com/technology/2018/nov/14/google-betrays-patient-trust-deepmind-healthcare-move,
20. https://techcrunch.com/2019/09/19/google-completes-controversial-takeover-of-deepmind-health/
21. Kit Huckvale, John Torous and Mark Larsen, 'Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation', JAMA Netw Open;2(4) e:192542. Doi:10.1001/jamanetworkopen.2019.2542
22. https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/
23. Dongwoon Han, 'Current Status of Electronic Medical Record Systems in Hospitals and Clinics in Korea', Healthcare Informatics Research 23(3) 189-196, July 2017, DOI: 10.4258/hir.2017.23.3.189
24. http://www.koreabiomed.com/news/articleView.html?idxno=4735
25. Casey Ross and Ike Swetlitz, 'IBM's Watson computer recommended "unsafe and incorrect" cancer treatments, internal documents show', StateNews, July 2018, https://www.statnews.com/wp-content/uploads/2018/09/IBMs-Watson-recommended-unsafe-and-incorrect-cancer-treatments-STAT.pdf.
26. http://www.koreabiomed.com/news/articleView.html?idxno=5776
27. https://publicservices.international/resources/news/korea-khmu-campaigns-against-for-profit-hospitals
28. Stephanie Dutchen, 'The Importance of Nuance', Harvard Medicine, Autumn 2019, https://hms.harvard.edu/magazine/artificial-intelligence/importance-nuance
29. https://www.hinz.org.nz/news/479973/The-inconvenient-truth-about-AI-in-health.htm
30. https://9to5mac.com/2018/08/02/south-korea-apple-tax/
31. http://www.koreaherald.com/view.php?ud=20190109000615
32. https://www.bloomberg.com/news/articles/2018-10-09/samsung-family-s-4-billion-tax-strategy-dragged-into-spotlight
33. https://www.healthline.com/health-newsis-da-vinci-robotic-surgery-revolution-or-ripoff-021215#3
34. https://www.therobotreport.com/intuitive-surgical-opens-korean-innovation-training-center/
35. https://www.worldbank.org/en/topic/digitaldevelopment/brief/smart-cities
36. https://www.aiib.org/en/policies-strategies/operational-policies/sustainable-cities/.content/_download/sustainable-cities-strategy.pdf
37. https://www.straitstimes.com/

singaporesingapore-is-worlds-smartest-city-imd-smart-city-index
38. Gaurav Dwivedi, Smart Cities Mission in India. Footprints of International Financial Institutions, July 2019, Centre for Financial Accountability, New Delhi, pp. 17-18; see also http://timesofindia.indiatimes.com/india/Sushma-seeks-Singapore-expertise-for-smart-cities/articleshow/40320200.cms
39. http://smartcities.gov.in/content/
40. http://smartcities.gov.in/content/innerpage/smart-city-features.php
41. https://economictimes.indiatimes.com/news/company/corporate-trends/37-companies-get-land-to-set-up-units-under-delhi-mumbai-industrial-corridor-project/articleshow/63003599.cms?from=mdr
42. Sang Keon Lee, Heeseo Rain Kwon, HeeAh Cho, Jongbok Kim, Donju Lee, International Case Studies of Smart Cities: Songdo Republic of Korea, IDB/Koreaa Research Institute for Human Settlements, October 2016, https://esci-ksp.org/wp/wp-content/uploads/2016/10/International-Case-Studies-of-Smart-Cities-Songdo-Republic-of-Korea.pdf.
43. https://wonderfulengineering.com/40-billion-city-south-korea-becomes-ghost-investment-runs/.
44. https://www.scmp.com/week-asia/business/article/2137838/south-koreas-smart-city-songdo-not-quite-smart-enough
45. Ayona Datta, 'New urban utopias of postcolonial India: "Entrepreneurial urbanization" in Dholera smart city, Gujarat', 5(1) Dialogues in Human Geography, 2015, 3-22 at 10.
46. https://www.alphabeta.com/our-research/the-digital-komodo-dragon-how-indonesia-can-capture-the-digital-trade-opportunity-at-home-and-abroad/
47. https://smartcitiescouncil.com/article/developing-smart-province-indonesia-opportunity-collaborate
48. https://smartcitiescouncil.com/member-levels/global-lead-partners
49. https://anz.smartcitiescouncil.com/article/meet-executive-director
50. https://smartcitiescouncil.com/article/readiness-network
51. http://mohua.gov.in/cms/smart-cities.php
52. S.R. Chowdury, 'As Bhopal is recast as a Smart City, its poor have a question: where's the room for us?', Scroll.in, 28 January 2019, https://scroll.in/article/910434/as-bhopal-is-recast-as-a-smart-city-poor-residents-worry-if-they-will-have-a-place-in-it
53. https://www.scoop.co.nz/stories/HL1912/S00115/surveillance-fears-over-plans-to-put-sensors-in-state-houses.htm
54. World Bank, World Development Report 2016. Digital Dividends, Washington DC, 240-241
55. https://www.theguardian.com/commentisfree/2012/dec/04/smart-city-rio-songdo-masdar; https://www.nytimes.com/2005/10/05/technology/techspecial/koreas-hightech-utopia-where-everything-is-observed.html
56. https://www.innovationiseverywhere.com/why-is-singapore-the-smartest-city-in-the-world/
57. https://www.stuff.co.nz/technology/107362458/government-agencies-turn-to-google-spark-data-to-try-and-solve-aucklands-traffic-woes
58. Ayona Datta, 4-5
59. Sang Keon Lee, et al.
60. https://iecetech.org/index.php/Technology-Focus/2019-02/Cyber-attacks-targeting-critical-infrastructure
61. https://qz.com/940660/tech-is-overwhelmingly-male-and-men-are-just-fine-with-that/
62. https://www.cio.com/article/3432144/inside-singapore-s-national-digital-identity-programme.html
63. https://www.biometricupdate.com/201810/singapore-launches-biometric-app-for-secure-digital-govt-transactions
64. https://www.channelnewsasia.com/news/singapore/singpass-mobile-app-login-government-e-services-fingerprint-face-10651414
65. United Kingdom National Audit Office, Investigation into Verify, 5 March 2019, https://www.nao.org.uk/wp-content/uploads/2019/03/Investigation-into-verify.pdf
66. https://www.forbes.com/sites/thomasbrewster/2019/07/04/london-police-facial-recognition-fails-80-of-the-time-and-must-stop-now/#548a62afbf95
67. http://time.com/5409604/india-aadhaar-supreme-court/
68. Interview conducted by Mary Ann Manahan, 11 June 2019
69. https://scroll.in/article/910434/as-bhopal-is-recast-as-a-smart-city-poor-residents-worry-if-they-will-have-a-place-in-it
70. ILO, Organising Informal Economy Workers into Trade Unions, ILO/ACTRAV, 20 June 2019, https://www.ilo.org/actrav/media-center/pr/WCMS_711217/lang--en/index.htm
71. Ayona Data, 15
72. http://ncrhomes.com/2011/delhi-mumbai-corridor-7-new-smart-cities-coming/
73. https://india.smartcitiescouncil.com/article/about-us-india
74. https://www.thehindubusinessline.com/specials/india-file/whats-smart-about-smart-cities/article26367835.ece
75. https://india.mongabay.com/2019/08/amaravati-capital-city-project-from-utopia-to-an-uncertain-future/
76. https://www.cenfa.org/publications/booklet-smart-cities-mission-in-india-footprints-of-ifis/

PUBLIC SERVICES
INTERNATIONAL
The global union federation of workers in public services

45 AVENUE VOLTAIRE, BP 9
01211 FERNEY-VOLTAIRE CEDEX
FRANCE

TEL: +33 4 50 40 64 64
E-MAIL: PSI@WORLD-PSI.ORG
WWW.PUBLICSERVICES.INTERNATIONAL

Public Services International is a Global Union Federation of more than 700 trade unions representing 30 million workers in 154 countries. We bring their voices to the UN, ILO, WHO and other regional and global organisations. We defend trade union and workers' rights and fight for universal access to quality public services.