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

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 exploiting 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

©The Conversation, CC BY-NC

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

© PSI 2017

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

© Shutterstock 2020

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 'maliciious 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.

© Shutterstock 2020

- 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[20].

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[18]. 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[19].

- **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].

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 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.

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[26]. 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.

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

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. Meganational 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].

4. “Smart Cities”

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.

© Shutterstock 2020

‘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[36].

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[38]. 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.[51]”

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'[55].

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[56]."

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[58]."

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.

© Shutterstock 2020

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[59]."

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.

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]."

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 infrastructure 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.

India's mass data profiling deemed constitutional: The Indian government's Aadhaar biometric 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].

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.

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.

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.

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[67]."

SOCIAL WELL-BEING

'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.

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[68]."

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

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].

‘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.

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].

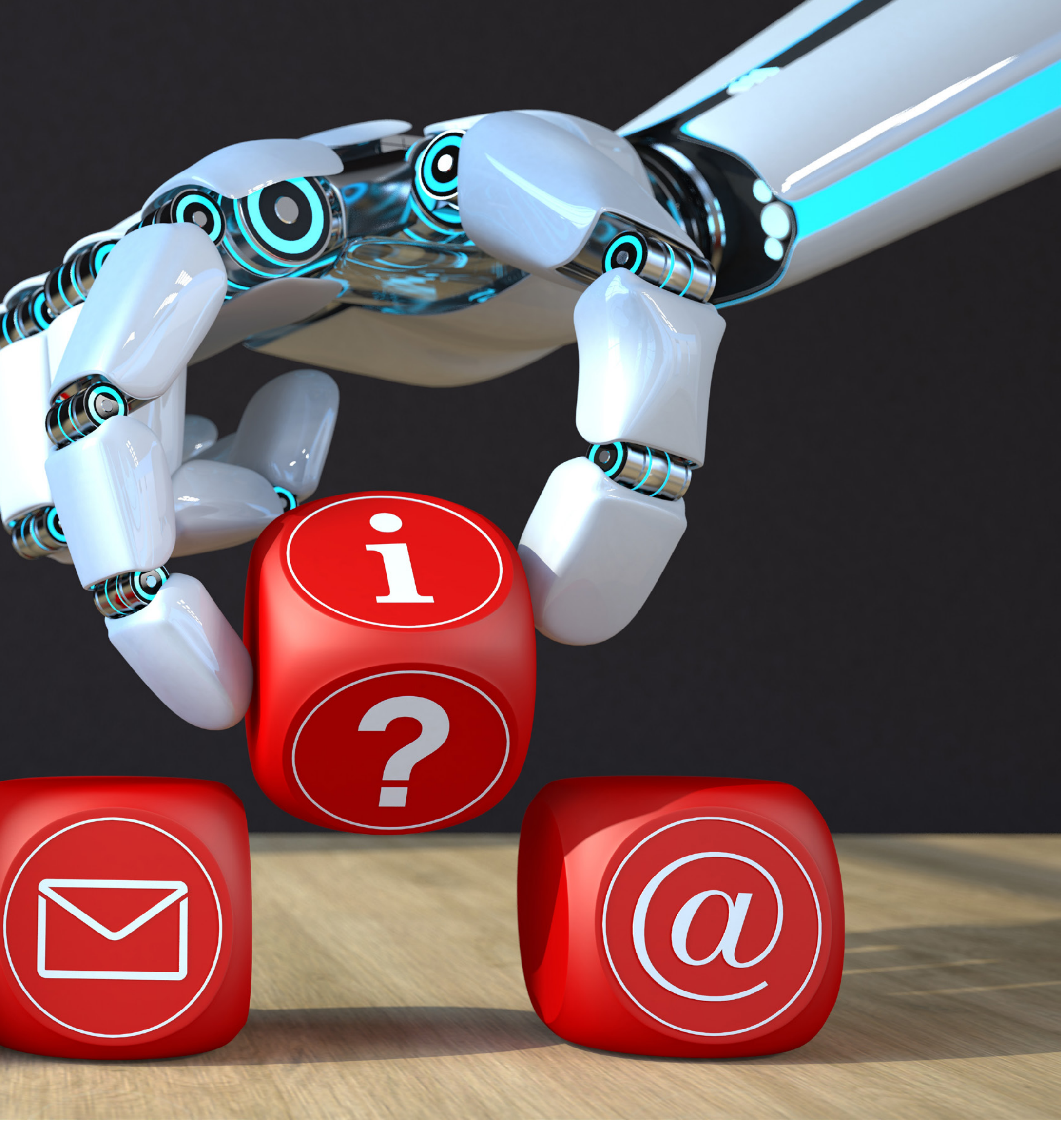
5. Recommendations

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.



© Shutterstock 2020

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) 189-198, 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-10851414

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.