Increased Uptake of Surveillance Technologies During COVID-19

Implications for Democracies in the Global South

Alex Read[*]

Abstract

Social change and introduction of new technologies have historically followed crises such as pandemics, and COVID-19 has seen increasing public tracking through the use of digital surveillance technology. While surveillance technology is a key tool for enhancing virus preparedness and reducing societal risks, the speed of uptake is likely to raise ethical questions where citizens are monitored and personal data is collected. COVID-19 has occurred during a period of democratic decline, and the predominant surveillance-based business model of the 'platform economy', together with the development and export of artificial intelligence (AI)-powered surveillance tools, carries particular risks for democratic development in the countries of the Global South. Increased use of surveillance technology has implications for human rights and can undermine the individual privacy required for democracies to flourish. Responses to these threats must come from new regulatory regimes and innovations within democracies and a renewed international approach to the threats across democracies of the Global North and South.

Keywords: surveillance technology, platform economy, COVID-19, democracy, global south, belt and road initiative.

A Introduction

Much media coverage of the COVID-19 pandemic has represented the pandemic and responses to it as being unprecedented; however, in many ways this is not the case. Historically, crises such as pandemics have met with rapid social change and accelerating trends in healthcare and technology. The Spanish flu of 1918-1919 transformed public health in many countries, introducing socialized healthcare and systems of disease tracking. Much earlier on, the black death of the 14th and 15th centuries in Europe unravelled the feudal system and ushered in various labour-saving technologies for better or worse, including clocks and the printing press, crossbows and guns. Surveillance is a core function of public health services, and what is unprecedented during the COVID-19 pandemic is the ability

* Alex Read, democratic governance consultant for organisations including UNDP, Inter-Parliamentary Union, Westminster Foundation for Democracy.

European Journal of Law Reform 2020 (22) 4
doi: 10.5553/EJLR/138723702021022004009

of modern digital technologies to enable 'bio-surveillance', integrating public health surveillance with techniques employing big data.[1] The changes introduced following a crisis such as a pandemic build onto the social, political and economic contexts of the time, and COVID-19 is occurring in a vastly more networked and connected digital world. It is also a world in which democratic governance is showing signs of decline.

The Varieties of Democracy Institute (V-Dem) has shown that for the first time since 2001 "there are more autocracies than democracies in the world".[2] Using a multidimensional dataset that examines indicators across five high-level principles of democracy – electoral, liberal, participatory, deliberative and egalitarian – in 2019 democracy was seen to have declined in 26 countries, and, for the first time since 2001, autocracies were in the majority. However, amidst a degree of democratic backsliding there is growing popular demand for democratic governance in many states. V-Dem data showed that pro-democracy protests "reached an all-time high in 2019".[3]

The International Institute for Democracy and Electoral Assistance (IDEA) reported that in 2019 democracies expanded global reach but that there was a decline in the qualities that make for strong democracies such as popular control over public decision-making and decision makers and equality between citizens in the exercise of that control.[4] Autocratization in certain countries has involved reduced scope for civil society and academia, restricted ability to protest, the use of polarizing messages by governments to mobilize populations around an illiberal agenda, assaults on freedom of expression and the media and, in some cases, decline in the standards of free and fair elections.[5]

IDEA has asserted that the erosion of democracy has been "exacerbated by polarisation, disinformation and hate speech"[6] propagated on digital platforms, highlighting the ongoing transformation of societies in the digital era. The adoption of digital technology in our lives has in many ways been empowering and has led to democratic progress. It has transformed the public sphere and advanced political communication, providing platforms for self-expression and tools for citizens to voice opinions and mobilize across the world. Technologies have enhanced representative government by providing additional avenues for

1 Danielle L. Couch, Priscilla Robinson and Paul A. Komesaroff, 'COVID-19—Extending Surveillance and the Panopticon', *Journal of Bioethical Inquiry*, 2020, http://link.springer.com/10.1007/s11673-020-10036-5 [accessed 17 October 2020].

2 Garry Hindle, Staffan I. Lindberg, Anna Lührmann, Seraphine F. Maerz, Sandra Grahn, Nazifa Alizada, Lisa Gastaldi, and Sebastian Hellmeier, *Autocratization Surges – Resistance Grows. Democracy Report 2020*, 2020.

3 *Ibid*.

4 International IDEA, *The Global State of Democracy 2019: Addressing the Ills, Reviving the Promise*, *The Global State of Democracy 2019: Addressing the Ills, Reviving the Promise*, 2019.

5 Hindle, Lindberg, Lührmann, Maerz, Grahn, Alizada, Gastaldi, and Hellmeier, *Autocratization Surges – Resistance Grows. Democracy Report 2020*.

6 International IDEA, *The Global State of Democracy 2019: Addressing the Ills, Reviving the Promise*.

citizen participation, bridging the gap between decision makers and citizens.[7] However, there are increasing concerns of risks to democracy from digital technology. Disinformation on social media has been attributed as a factor in democratic decline, manipulating public opinion and affecting credibility and trust in political processes.[8] On leaving office, President Obama spoke of people growing isolated by competing 'facts' and that social media had enabled a 'dust cloud of nonsense'.[9]

Public trust in government and institutions is critical during a pandemic. COVID-19 has seen many countries attempting to impose extraordinary restrictions around freedom of movement and tracking of the public, with democratic governments attempting a delicate balance between introducing measures to safeguard public health and the economy and protecting civil liberties. In the urgency of reducing the spread of the virus and reopening economies, many governments have sought out and introduced new technologies to track infections, control lockdowns and monitor the movement of people. The introduction of technologies for public surveillance can be a key tool in enhancing virus preparedness and contributing to disaster risk reduction. However, in many cases introduction of new technology has occurred under emergency measures, and the speed of uptake is likely to not only cross new technical boundaries but also raise ethical questions as citizens are monitored and personal data is collected. Once introduced, the widespread use of surveillance technologies might be difficult to reverse. Democratic institutions are critical to ensuring that measures taken are responsive to rights and civil liberties concerns, but with many parliaments restricting functions or moving to virtual ways of working, there are risks of their being sidelined at a time when they are most needed.

This article will examine trends in two forms of surveillance in the digital era – surveillance in the online 'platform economy' and the development of surveillance technologies using AI. It will examine links between the two and assess how emergency measures under COVID-19 may lead to accelerated uptake and societal changes. It will assess the ways in which these modern tools of surveillance represent a threat to democracy, focusing on countries in the Global South,[10] and propose measures that democratic countries can take domestically and internationally to address potential risks, drawing lessons for the promotion of international democratic governance.

7 *Ibid*.

8 *Ibid*.

9 Taylor Owen, 'The Case for Platform Governance', *CIGI Papers*, 231, 2019.

10 Defined as "regions outside Europe and North America, mostly (though not all) low-income and often politically or culturally marginalized. The use of the phrase Global South marks a shift from a central focus on development or cultural difference toward an emphasis on geopolitical relations of power". Nour Dados and Raewyn Connell, 'The Global South', *Context*, 11 February 2012, 2012, 12-13.

European Journal of Law Reform 2020 (22) 4
doi: 10.5553/EJLR/138723702021022004009

B Surveillance and the Platform Economy

The term 'platform economy' is used to describe a 'rapidly reorganizing global economy' in which online structures created by companies such as Amazon, Facebook and Google are enabling 'a wide range of human activity' and changing ways of working, socializing and creating economic value.[11] The primary business model employed by these companies involves extraction and analysis of users' data. Algorithms are used to sort and aggregate vast amounts of data produced online, assign profiles to individuals and predict their interests and behaviour. This is sold to advertisers for targeting.[12]

The value of the platform economy lies in the data extracted. An increasing amount of data enables the training of machine learning models that, in turn, can produce better behavioural predictions and increase advertising revenue.[13] The model prioritizes "capturing our attention and providing free services, information and entertainment in order to resell our attention to advertisers".[14] This quest for increasing amounts of data leads to companies seeking to render into data many aspects of the world that have not been quantified before.[15] Increasingly, expansion is taking place into the offline world, with internet-of-things devices and innovations like smart cities moving private and public interaction into the online space.

Data collected can reveal raw facts about individuals and, when processed, can identify underlying thoughts, behaviours and identities. Metadata collected on, for example, email recipients, location records and the timestamp on emails and photos can be used to provide insights into "an individual's behaviour, social relationship, private preference and identity that go beyond even that conveyed by accessing the content of a communication".[16] AI and machine learning can understand detailed characteristics about people and aggregate them into specific groupings. This can be used to infer information such as sexual identify, political views and personality traits and to predict behaviour on a population scale using algorithmic models.[17]

The ability to collect granular level of detail on individuals has enabled what is called 'persuasion architectures' that can influence behaviour.[18] The case of

11 Martin Kenney, Dafna Bearson and John Zysman, 'The Platform Economy Matures: Pervasive Power, Private Regulation, and Dependent Entrepreneurs', *SSRN Electronic Journal*, 2019.
12 Soshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs, 2019).
13 Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights* (London, 2019).
14 Yuval Noah Harari, 'Why Technology Favors Tyrrany', *The Atlantic,*www.theatlantic.com/magazine/archive/2018/10/yuval-noah-harari-technology-tyranny/568330/.
15 Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights*.
16 *Ibid*.
17 *Ibid*.
18 *Ibid*.

Cambridge Analytica demonstrated the way in which campaigns use data about voters and analysis of personality to enable micro-targeting of political messages that can exploit prejudices. There is increasing concern that 'deep fake' technologies that manipulate video and audio using AI, when combined with personalized data "will enable individualized versions of events, indistinguishable from reality and designed on personal beliefs and biases, to be delivered directly into our social feeds".[19] Targeting of misinformation based on techniques of online surveillance threatens the credibility of information that democracies rely on. This shaping of reality will only get more challenging as our digital spaces become home to increasingly sophisticated automated bots and agents.[20]

In countries in the Global South such as Myanmar and the Philippines, "70 percent of all internet traffic flows through either a Google or Facebook server".[21] Facebook and Google have expanded into the Global South, for example through Facebook's 'free basics' programme, which channels internet traffic through Facebook's servers, collecting data on the use of third-party services.[22] Privacy International investigated low-cost mobile phones produced for the Philippines market using Google's Android operating system, finding that they lacked adequate security and "exposed users' data to potential exploitation by scammers, political parties and government agencies".[23] For many internet users in the Global South, "these companies are the internet",[24] leaving them susceptible to mass surveillance and exploitative data practice.

At a global level, there is an increasing divide between the big data rich and poor. The concentration of a small number of companies in data-driven sectors gives them the opportunity to transform raw data from products sold in the Global South into value-added data products. These products and services generate more data, which perpetuates their market advantage. Developing countries may not yet see data as a resource, and without greater understanding of the economic and political use of data, officials may not understand how to protect citizens' interests.[25] It has been argued that this constitutes a new 'digital colonialism' as "knowledge, authority, and power to sort, categorise, and order human activity rests with the technologist, for whom [populations of the Global South] are merely data-producing 'human natural resources'".[26] While there has been a very

19 Robert Chesney and Danielle Keats Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security', 107 California Law Review 1753 (2019).
20 Owen, 'The Case for Platform Governance'.
21 *Ibid*.
22 Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights*.
23 Privacy International, 'Buying a Smart Phone on the Cheap? Privacy Might Be the Price You Have to Pay', https://privacyinternational.org/long-read/3226/buying-smart-phone-cheap-privacy-might-be-price-you-have-pay [accessed 30 August 2020].
24 Owen, 'The Case for Platform Governance'.
25 Susan Ariel Aaronson, 'Data Is a Development Issue', *CIGI Papers*, 223, 2019, 1-32.
26 Abeba Birhane, 'Algorithmic Colonisation of Africa', *The Elephant*, 2020, www.theelephant.info/long-reads/2020/08/21/algorithmic-colonisation-of-africa/ [accessed 25 August 2020].

European Journal of Law Reform 2020 (22) 4
doi: 10.5553/EJLR/138723702021022004009

rapid growth of use of digital technologies and online connectivity worldwide, debates on issues such as surveillance, privacy and internet neutrality are commonly framed from the perspective of Western contexts and behaviour of users, which can result in the extension of "new forms of market governance over the informal poor, reconfiguring their habits, social practices, and economic strategies under the banner of poverty reduction".[27]

The risks to democracy are becoming clear in countries in the Global South. In the Philippines, around 96% of the population who are on the internet are on Facebook, one of the highest rates of users in the world.[28] During the 2016 election there was evidence that public opinion can be shaped using digital tools of micro-targeting and viral disinformation. The media organization Rappler identified a barrage of propaganda and fake news put out by bots, fake accounts and anonymous pages on Facebook prior to the 2016 election, an election notable for its angry and divisive political discourse. Facebook's opaque algorithms were seen as contributing to shaping reality and echo chambers harmful to democracy.[29] In Myanmar, fake accounts on Facebook posted disinformation associated with inciting violence in 2017 against the Rohingya Muslim minority group. The unregulated nature of the platform has been described by a civilian MP as "dangerous and harmful for our democratic transition".[30] In India, public organization has been stifled by restricting access to the internet and cell phone communication. These cases demonstrate how big tech can be 'weaponized' by states and other actors with anti-democratic motivations.[31]

Democracy requires informed citizens to legitimize collective governance and in the face of these risks, understanding how online platforms shape and influence the quality of information we receive is critical to upholding democracy. Disinformation undermines participation in a democratic society, which requires well-informed citizens and objective information as the basis for public deliberation and for holding institutions accountable. The use of online platforms to spread such disinformation has been viewed as resulting in

> a fragmenting public sphere [that] has catalysed the polarization of society into adversarial 'tribes' [....] and the collapse of the civic virtues that were

27 Payal Arora, 'The Bottom of the Data Pyramid: Big Data and the Global South', *International Journal of Communication* vol.10 (2016).

28 Maria A. Ressa, 'Propaganda War: Weaponizing the Internet', *Rappler*, 2016, https://rappler.com/nation/propaganda-war-weaponizing-internet [accessed 30 August 2020].

29 *Ibid*.

30 The New York Times, 'A Genocide Incited on Facebook, With Posts From Myanmar's Military', www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html [accessed 28 August 2020].

31 Bernard Arogyaswamy, 'Big Tech and Societal Sustainability: An Ethical Framework', *AI and Society*, 2020, 12.

> once held to be essential to a democratic polity, such as tolerance, integrity, truthfulness and responsibility.[32]

Often, the effects rather than causes are focused on. Disinformation has a severe impact on democracy; however, it is not the case of the digital tools themselves being illiberal but the underlying logic and surveillance-based business model behind them. Facebook and other platforms optimize for engagement on the platform rather than for truth and, to enable this, prioritize viral content above objective and balanced news. In the case of the Philippines this was seen as replacing "editorial, funding and distribution systems of the free press" with "algorithms and incentives of the newsfeed".[33] This creates the conditions in which information can be manipulated, facts questioned and propaganda and misinformation micro-targeted to people seen as amenable. Democratic institutions have not been able to keep pace, enabling the rise of populist leaders who can then "gain control as society gets further splintered apart, and then use formal powers given to them by governments".[34]

COVID-19 has been seen as strengthening the key actors in the platform economy. The big tech platform companies have increased their wealth considerably during the pandemic as the global economy increasingly moves online. Despite the expected economic impact of lockdowns, Apple, Amazon and Facebook's market value in the second quarter of 2020 increased by a combined quarter trillion dollars, more than the GDP of New Zealand.[35] COVID-19 has exacerbated concerns about

> the nature and extent of the power exercised through big data analytics, the identity of those on whose behalf such power was exercised, and to whom – if anyone – they were accountable.[36]

The technology sector has also been increasingly drawn upon to support governments to control the virus and help reopen economies. Contact tracing apps are being used in around 80 countries, many of the apps collecting personally identifiable information and health records.[37] An analysis of 30 out of 50 apps indicated that they require access to users' mobile devices, including

32 Fukuyama 2018, in International IDEA, *The Global State of Democracy 2019: Addressing the Ills, Reviving the Promise*.

33 Taylor Owen, 'Maria Ressa and Social Media's Illiberal Intent ~ Centre for International Governance Innovation', *CIGI Online*, 2020, www.cigionline.org/articles/maria-ressa-and-social-medias-illiberal-intent [accessed 30 August 2020].

34 *Ibid*.

35 Carmen Reinicke, 'Facebook, Apple, and Amazon Add a Combined $ 274 Billion in Market Value Following Earnings ~ Markets Insider', *Markets Insider*,https://markets.businessinsider.com/news/stocks/facebook-apple-amazon-alphabet-stock-price-add-market-value-earnings-2020-7-1029455838# [accessed 30 August 2020].

36 Couch, Robinson and Komesaroff, 'COVID-19—Extending Surveillance and the Panopticon'.

37 Tanusree Sharma and Masooda Bashir, 'Use of Apps in the COVID-19 Response and the Loss of Privacy Protection', *Nature Medicine*, 2020, 19-20.

European Journal of Law Reform 2020 (22) 4
doi: 10.5553/EJLR/138723702021022004009

"contacts, photos, media, files, location data, camera, the device ID, call information, the Wi-Fi connection, full network access, the google service configuration".[38] Only 16 of 50 apps indicated that data was encrypted and reported only in an aggregated format. Location surveillance introduced during COVID-19 has also seen telecoms companies being drawn on to share data on an unprecedented scale, raising significant privacy and civil liberties concerns.[39]

In 2020, a small number of big tech corporations control platforms, manage vast amounts of information and are spearheading research into AI and algorithms. Yet so far technology is a highly unregulated economic sector owing in part to the rapid pace of change.[40] While the General Data Protection Regulation in Europe and national initiatives such as India's proposed Data Protection Law offer prospects of more robust regulatory regimes, the key players in the platform economy have, in the main, existed outside of formal accountability channels. It is incumbent on mature democracies to understand and attempt to address the harmful effects of the surveillance-based platform economy that has proven damaging to democracies in the Global South.

C State Surveillance

Technological breakthroughs such as maturation of machine learning, cloud computing, online data collection and improvements in microchips and hardware are rapidly expanding the scope and application of AI, yielding applications that will rapidly change societies. AI is already embedded in apps and websites with widespread application of innovations such as self-driving cars and automated manufacturing expected across the economy in coming years. AI expert Kai Fu Lee asserts that "these uses are full of both promise and potential peril, and we must prepare ourselves for both".[41]

These capabilities are increasingly being rolled out in countries worldwide, transforming the abilities of governments. Surveillance technologies using AI include smart city platforms that use data collected from numerous sensors in the urban environment to manage resources and target services and safe city platforms that use hardware such facial recognition surveillance cameras with AI analytics to predict and prevent crime. For example, in the United States AI is used for predictive policing that identifies areas where crime is expected to occur.[42] Surveillance using AI can be conducted in an automated way, casting a

38 *Ibid*.

39 *Ibid*.

40 Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights*.

41 Kai Fu Lee, *AI Superpowers: China, Silicon Valley and the New World Order* (Boston: Houghton Mifflin Harcourt, 2018).

42 Steven Feldstein, 'The Global Expansion of AI Surveillance', *Carnegie Endowment for International Peace*, September, 2019, 1-42.

much wider net than traditional surveillance.[43] This type of technology has considerable potential to create efficiencies and improve the lives of citizens, reducing crime and making cities and countries safer. However, it will also offer increasing capabilities to monitor, understand and control citizens, and, in the hands of oppressive regimes, could be used to constrain opposition and maintain power.

Use of surveillance technologies is already prevalent worldwide, with "51 percent of advanced democracies [deploying] AI surveillance systems".[44] For autocratic regimes it also offers opportunities to tighten social control. Research has shown that "37 percent of closed autocratic states, 41 percent of electoral autocratic/competitive autocratic states, and 41 percent of electoral democracies/illiberal democracies deploy AI surveillance technology" and that "governments in autocratic and semi-autocratic countries are more prone to abuse AI surveillance than governments in liberal democracies".[45] Countries in authoritarian systems with low political rights are investing heavily in AI surveillance, expanding facial recognition and analytics that enable sophisticated public monitoring in the Gulf, East Asia and South/Central Asia.[46] It gives the potential for regimes with less rigorous privacy and data protection standards to aggregate and analyse various forms of data on individuals, such as medical records, criminal records, bank statements, online activity, biometric data and physical information from location and CCTV data.

Currently, the most prominent example of surveillance technology being used for repressive purposes is in China's Xinjiang province. There is evidence that one million Muslim Uighurs are the target of a comprehensive population monitoring programme using modern technologies. Biometric data, including DNA, iris scans and facial imagery, have been collected, with AI-powered surveillance equipment used to track the population.[47]

> Uighurs can travel only a few blocks before encountering a checkpoint outfitted with one of Xinjiang's hundreds of thousands of surveillance cameras. Footage from the cameras is processed by algorithms that match faces with snapshots taken by police at "health checks." At these checks, police extract all the data they can from Uighurs' bodies. They measure height and take a blood sample. They record voices and swab DNA.[48]

Xinjiang has provided a glimpse of capabilities that may be rolled out nationwide. CETC, the state-owned company engaged in setting up much of the surveillance

43 *Ibid*.
44 *Ibid*.
45 *Ibid*.
46 *Ibid*.
47 Amnesty International, *Out of Control: Failing EU Laws for Digital Surveillance Export* (London, UK, 2020).
48 Ross Andersen, 'The Panopticon Is Already Here', *The Atlantic*, 2020, www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/ [accessed 30 August 2020].

European Journal of Law Reform 2020 (22) 4
doi: 10.5553/EJLR/138723702021022004009

system in Xinjiang, is piloting projects in Zhenjiang, Guangdong and Shenzen. Companies such as SenseTime, CloudWalk, Megvii, Hikvision, iFlytek and Meiya Pico have also been involved in establishing the surveillance systems in Xinjiang.[49]

China's AI Development Plan outlines the ability to "grasp group cognition" and states that "AI brings new opportunities for social construction".[50] "Skynet"[51] and "Sharp Eyes"[52] are two mass surveillance projects that use biometric technology to enable the "monitoring, tracking, classification, and identification of individuals".[53] In China there are few checks on government power and on safeguards on handling and use of personal data.[54] As private firms in China are statutorily obliged to assist intelligence services, there are no hard barriers to integration of data for the state's use.[55] With big data collection and AI-powered technologies, the type of centralized database that exists on Chinese citizens has the potential to be "a formidable instrument of surveillance and oppression".[56]

In the future AI may offer the capability to match surveillance of every person entering a public space against data from, for example, communication records, travel records, friends and associates, reading habits and purchases. Many cities in China have developed 'safe city' platforms using 'city brains' that synthesize data from numerous sensors in an urban environment. It has considerable potential to help with public services such as transport and refuse but can also lend itself to integrated surveillance. This could predict signs of unrest, offering the government a political stranglehold on the public. The next generation of digital technology and AI could enable the state to "identify and quash opposition in advance by combining clues from its many channels of mass information collection".[57] However, this is not an issue confined to China, and many states are grappling with the question of how to prevent the emergence of "a public-private surveillance state".[58]

49 *Ibid*.
50 *Ibid*.
51 A project that started in 2005 involving the installation of cameras and video control centres in cities across China. Over 20 million cameras were in use by 2017, and the project increasingly incorporates use of facial recognition cameras.
52 A project that began in 2015 and that builds on Skynet, Involving the integration of public and private cameras into one police network. The plan calls for government bodies from local Communist Party of China committees upwards to participate in creating an "omni-present, fully networked, always working and fully controllable" system, incorporating facial-recognition technology. Xiao Qiang, 'President XI's Surveillance State', *Journal of Democracy*, 30/1 (2019), 53-67.
53 Amnesty International, *Out of Control: Failing EU Laws for Digital Surveillance Export*.
54 Qiang, 'President XI's Surveillance State', 53-67.
55 Andersen, 'The Panopticon Is Already Here'.
56 Qiang, 'President XI's Surveillance State', 53-67.
57 *Ibid*.
58 Andersen, 'The Panopticon Is Already Here'.

Surveillance technology is increasingly being exported to countries in the Global South. Countries signing up to China's Belt and Road Initiative (BRI) have received support for infrastructure such as new cities, high-speed rail and port infrastructure worldwide, but the BRI has also proven to be a means of export of surveillance technology through the use of soft loans to encourage purchases. Research has shown that at least 75 of 176 countries are using AI for surveillance, including smart city/safe city platforms, facial recognition and smart policing. China is driving AI surveillance, with Chinese companies Huawei and ZTE supplying AI surveillance systems to 63 countries, 36 of which are part of the BRI. Of 90 countries with regime types categorized as 'authoritarian to flawed democracies', Chinese companies are exporting AI surveillance technology to 54.[59]

In Bonifacio Global City in the Philippines, high-definition internet-connected cameras provide "24/7 intelligent security surveillance with data analytics to detect crime and help manage traffic".[60] The Zimbabwean government signed a strategic cooperation framework agreement with a Chinese start-up, CloudWalk Technology, for a large-scale facial recognition program, allowing CloudWalk to improve its underlying algorithms with more data on a wider range of facial types.[61] In Singapore, Sri Lanka and Mongolia, Chinese companies are providing AI-assisted surveillance and facial recognition cameras. Cities in Kenya, Uganda and Mauritius are being built with Chinese-made surveillance networks. Zambia is procuring over US$ 1 billion in telecoms equipment with internet-monitoring technology.[62]

However, China is not alone; Israel, France, the United Kingdom and the United States are also supplying advanced capabilities from location-tracking spyware and high-resolution video surveillance to hacking software and censorship filtering applications.[63] AI surveillance technology is being provided by US companies in 32 countries, primarily by ICM, Palantir and Cisco.[64] An example is Saudi Arabia, in which Huawei is supporting safe city projects, but

> Google is establishing cloud servers, UK arms manufacturer BAE has sold mass surveillance systems, NEC is vending facial recognition cameras, and Amazon and Alibaba both have cloud computing centres in Saudi Arabia and may support a major smart city project.[65]

59 Steven Feldstein, 'How Artificial Intelligence Systems Could Threaten Democracy', *Boise State University ScholarWorks*, 2019, 6.
60 *Ibid*.
61 Aaronson, 'Data Is a Development Issue', 1-32.
62 Andersen, 'The Panopticon Is Already Here'.
63 Steven Feldstein, 'When It Comes to Digital Authoritarianism, China Is a Challenge — But Not the Only Challenge - War on the Rocks', *War on the Rocks*, 2020, https://warontherocks.com/2020/02/when-it-comes-to-digital-authoritarianism-china-is-a-challenge-but-not-the-only-challenge/ [accessed 30 August 2020].
64 Feldstein, 'The Global Expansion of AI Surveillance', 1-42.
65 *Ibid*.

European Journal of Law Reform 2020 (22) 4
doi: 10.5553/EJLR/138723702021022004009

Amnesty International has found that companies in Europe, "Morpho (now Idemia), Axis Communications, and Noldus Information Technology – based in three different EU member states – France, Sweden, and the Netherlands" exported digital surveillance technology to China that was used by the Chinese public security bureau and other bodies for public surveillance.[66]

The UN Special Rapporteur on Freedom of Opinion and Expression has asserted that

> [t]he global surveillance industry [...] appears to be out of control, unaccountable and unconstrained in providing governments with relatively low-cost access to the sorts of spying tools that only the most advanced state intelligence services previously were able to use.[67]

The export of surveillance technologies has been criticized as enabling a "race to the bottom, in which liberal democratic governments continue to criticise the behaviour of others while using it to justify their own",[68] and there are significant questions about the extent to which democracies are placing safeguards on export and use of surveillance technology. The absence of effective regulatory regimes and oversight allows companies to "freely sell their technology to countries where human rights are not protected or respected".[69]

IDEA cites risks to democracy from autocratic regimes with global ambitions looking to export their models of governance.[70] The crisis has occurred at a time when the world's diplomatic relations are strained under the risk of the US and China decoupling in trade, technology, data and monetary arrangements. This may lead to competing systems of technology and governance standards around the use of technology. There are risks of China exporting technology with a geopolitical intent: to maintain dependence on Chinese technology and face pressure to align with China's agenda and to enable Chinese companies to gain access to data globally on which to train and refine AI systems.[71] This has implications for countries where democracy is fragile. As V-Dem highlighted, a positive sign in 2019 is that political protest is rising.[72] However, automated surveillance in the hands of autocrats could heavily undermine the ability of public political organization and opposition to autocratic rulers. While the use of surveillance technologies in itself is not necessarily repressive, the emergence of an authoritarian bloc of countries using these technologies could endanger the

66 Amnesty International, *Out of Control: Failing EU Laws for Digital Surveillance Export*.
67 *Ibid*.
68 Edin Omanovic, 'A Recipe for Hypocrisy: Democracies Export Surveillance Tech without Human Rights', *About:Intel*, 2020, https://aboutintel.eu/surveillance-export-human-rights/ [accessed 30 August 2020].
69 Amnesty International, *Out of Control: Failing EU Laws for Digital Surveillance Export*.
70 International IDEA, *The Global State of Democracy 2019: Addressing the Ills, Reviving the Promise*.
71 Feldstein, 'How Artificial Intelligence Systems Could Threaten Democracy', 6.
72 Hindle, Lindberg, Lührmann, Maerz, Grahn, Alizada, Gastaldi, and Hellmeier, *Autocratization Surges – Resistance Grows. Democracy Report 2020*.

political freedoms of billions of people and impact geopolitics throughout this century.

The COVID-19 pandemic has led to the rapid introduction of various surveillance technologies to track populations. In China, the United Arab Emirates and Qatar, algorithm-enabled risk scores in the form of a colour code allow people to enter venues, public spaces or use transport, using location and contacts to prove whether a person is healthy.[73] In China, two big providers of mobile payment systems, Alipay and WeChat, released apps that combine users' health, location and financial data to generate a personal infection risk rating.[74] The algorithms behind the codes can be opaque with questions relating to how codes are generated and whether results can be challenged. Trials on tech-enabled quarantine enforcement included facial recognition and CCTV, apps and bracelets and use of robotics. There have been high-profile cases of drones also being used for lockdown compliance in China, Rwanda, the UK, Portugal and Saudi Arabia, and other countries.[75] In Israel, drones have been reported checking through windows on people who tested positive for the virus.[76] Russia is reported to have deployed over 100,000 surveillance cameras and other forms of technology to enforce self-isolation.[77]

The move towards AI-enabled healthcare may catalyse the introduction of forms of biometric technology. US government and state agencies have examined the use of location data mining or facial recognition to trace infected people and to monitor and enforce isolation, working alongside companies such as Google, Facebook and controversial start-up Clearview AI.[78] China has robotics in place to screen patients using 5G-enabled thermometers as well as rings and bracelets connected to the CloudMinds AI platform to monitor changes in the body.[79] Some officials are suggesting that health tracking be expanded into areas such as

73 Khaleej Times, 'Have Doubts about UAE's New Covid-Tracing App? Here's Why It Is Safe, Private - News ~ Khaleej Times', 2020, www.khaleejtimes.com/coronavirus-pandemic/have-doubts-about-uaes-new-covid-tracing-app-heres-why-it-is-safe-private [accessed 30 August 2020].

74 Masha Borak, 'China Wants to Keep Health Codes after the Pandemic but Users Aren't so Sure ~ South China Morning Post', 2020, www.scmp.com/abacus/tech/article/3087437/china-wants-keep-health-codes-after-pandemic-users-arent-so-sure [accessed 30 August 2020].

75 Dimitri Tozmetkis and Morgan Meaker, 'Covid-19 Surveillance Tech Explained: 6 Ways Governments Are Monitoring the Virus – and You', *The Correspondent*, 2020, https://thecorrespondent.com/432/covid-19-surveillance-tech-explained-6-ways-governments-are-monitoring-the-virus-and-you/57132345600-6bf2dd7f [accessed 30 August 2020].

76 Joseph Krauss, 'Israeli Police Use Drones to Enforce Virus Quarantines, Raising Privacy Concerns ~ The Times of Israel', *The Times of Israel*, 2020, www.timesofisrael.com/israeli-police-using-drones-to-enforce-coronavirus-quarantines/ [accessed 30 August 2020].

77 Jelena Timotijevic, 'Society's "New Normal"? The Role of Discourse in Surveillance and Silencing of Dissent During and Post Covid-19', *SSRN Electronic Journal*, 2020, 1-18.

78 Rafael Calvo, Christoph Deterding and Richard Ryan, 'Health Surveillance during Covid-19 Pandemic: How to Safeguard Autonomy and Why It Matters', *Bmj*, 2020.

79 Tim Honiyak, 'How China Is Using Robots and Telemedicine to Combat the Coronavirus', *CNBC*, 2020, www.cnbc.com/2020/03/18/how-china-is-using-robots-and-telemedicine-to-combat-the-coronavirus.html, [accessed 30 August 2020].

European Journal of Law Reform 2020 (22) 4
doi: 10.5553/EJLR/138723702021022004009

sleep and smoking habits after the pandemic.[80] Ultimately, there is concern that the intrusion of AI-enabled biotech into people's lives will lead to the ability to understand individuals' emotions and thoughts.[81]

State surveillance poses a serious threat to democratic development and political pluralism. Those who are under constant surveillance feel pressure to conform. Additionally, it threatens freedom of expression and association and protection of minorities in autocratic countries. In the aftermath of COVID-19, it will be pertinent to ask how far surveillance techniques will become more regular features of daily life and normalized post-COVID.[82] There are also questions about how to dismantle the "technical and legal structures after the pandemic", unless those structures have safeguards in place that protect democratic rights and freedoms.[83]

D Democratic Responses to Threats From Surveillance Technologies

Liberal democracy is based on the core idea that there is "a sphere beyond the rightful reach of government in which individuals can enjoy independence and privacy".[84] Ultimately, the threats to democracy outlined previously come from a loss of privacy, the right to which is protected under Art. 12 of the United Nations Declaration on Human Rights (UDHR) and Art. 17 of the International Covenant on Civil and Political Rights (ICCPR).[85] The Office of the High Commissioner of Human Rights (OHCHR) has stated the following:

> Privacy can be considered as the presumption that individuals should have an area of autonomous development, interaction and liberty, a 'private sphere' with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals [...] This encompasses concepts of freedom of intrusion into private lives, the right to control information about ourselves, and the right to a space in which we can freely express our identities.[86]

Privacy is essential to autonomy and the ability to determine our identity, and the loss of privacy that new mechanisms of surveillance entail threatens both democracy and human rights. Amnesty International has asserted that "the

80 Borak, 'China Wants to Keep Health Codes after the Pandemic but Users Aren't so Sure ~ South China Morning Post'.
81 Harari, 'Why Technology Favors Tyrrany'.
82 Timotijevic, 'Society's "New Normal"? The Role of Discourse in Surveillance and Silencing of Dissent During and Post Covid-19', 1-18.
83 *Ibid*.
84 William Galston, 'The Populist Challenge to Liberal Democracy', *Journal of Democracy*, 29/2 (2018).
85 Amnesty International, *Out of Control: Failing EU Laws for Digital Surveillance Export*.
86 Office of the High Commissioner of Human Rights, *The Right to Privacy in the Digital Age* (New York, 2018).

surveillance-based nature of Google and Facebook's business model undermines [...] the very essence of privacy".[87] The collection, use and manipulation of personal data to understand, categorize and micro-target citizens implies an intrusion into private lives and the space in which people express their identity. It "threatens our ability to freely and independently develop and express thoughts and ideas and leaves us vulnerable to outside influence and control"[88].

Surveillance has important psychological consequences. If we know that we are being watched, we necessarily change how we behave. Research over decades has demonstrated that

> societies can only thrive in environments that satisfy basic psychological needs, including autonomy – a sense of having volition and choice in your actions. Surveillance can engender a sense of being controlled and be experienced as thwarting autonomy, with negative effects on motivation and wellbeing.[89]

If external surveillance becomes the condition of individual life, it is unlikely democracy can flourish as, ultimately, automated surveillance threatens the "right to shape and define who we are as autonomous individuals".[90]

In the words of the United Nations High Commissioner for Human Rights

> even the mere generation and collection of data relating to a person's identity, family or life already affects the right to privacy, as through those steps an individual loses some control over information that could put his or her privacy at risk,

with biometric data being particularly sensitive.[91] In public spaces, "[t]he right to privacy comes into play when a Government is monitoring a public space, such as a marketplace or a train station, thereby observing individuals".[92] In this respect, both the collection and the analysis of personal data by companies in the platform economy and the increased use of AI-powered surveillance technologies such as facial recognition threaten human rights and fundamental freedoms. COVID-19 emergency responses risk embedding these new tools of surveillance in many countries, and the threats to democracy and human rights from

87 Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights*.
88 *Ibid*.
89 Calvo, Deterding and Ryan, 'Health Surveillance during Covid-19 Pandemic: How to Safeguard Autonomy and Why It Matters'.
90 Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights*.
91 Amnesty International, *Out of Control: Failing EU Laws for Digital Surveillance Export*.
92 Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights*.

European Journal of Law Reform 2020 (22) 4
doi: 10.5553/EJLR/138723702021022004009

unchecked surveillance require a response within and across democratic countries.

I Response Within Democracies

The speed of change in science and technology has left regulatory frameworks lagging behind. Democracies should take steps to minimize social costs related to the data-driven economy and surveillance-based business model of big tech companies.[93] In mature democracies, powers to break up and regulate the technology giants and ensure a diverse media environment should be considered. Ultimately, this will require new legal frameworks, different regulatory paradigms, new institutional forms. New forms of public oversight will need to audit these technologies, mirroring health and safety regulations.[94]

Regulations preventing exploitation of personal data and the aggregation of data from various platforms that citizens engage with should be enacted to uphold privacy, as well as laws protecting sensitive data such as medical records from being exploited. Governments should be able to compel access to data from platform companies with substantial influence over the public.[95] This should be backed up by national discussions in democratic countries around human rights implications of surveillance and the ethical use of AI.[96] We need to change the perception that we are 'users' and engage in a public debate on the concept of 'who gets to know my experience'. Broad stakeholder collaboration and a national discussion about rights and access to data will be required on the subject of whether we want data to belong to "me, or the government, or to a corporation, or to the human collective"[97] alongside data protection laws that view access to and use of data as rights issues.[98]

Canada shows that a broad-based discussion can help to build public trust in the data-driven economy, holding round tables with over 580 participants and developing a digital charter based on 10 principles.[99] This type of national discussion will also be important to set ethics and regulations around the export of potentially harmful surveillance technologies from democratic countries.

The European Parliament has called on EU institutions and member states to protect against "the impact of intrusion and surveillance systems on human

93 Owen, 'The Case for Platform Governance'.
94 *Ibid*.
95 Aaronson, 'Data Is a Development Issue', 1-32.
96 Avi Marciano, 'The Discursive Construction of Biometric Surveillance in the Israeli Press: Nationality, Citizenship, and Democracy', *Journalism Studies*, 20/7 (2019), 972-90.
97 Harari, 'Why Technology Favors Tyrrany'.
98 Marciano, 'The Discursive Construction of Biometric Surveillance in the Israeli Press: Nationality, Citizenship, and Democracy', 972-90.
99 1. Universal Access; 2. Safety and Security; 3. Control and Consent; 4. Transparency, Portability and Interoperability; 5. Open and Modern Digital Government; 6. A Level Playing Field; 7. Data and Digital for Good (in an ethical manner); 8. Strong Democracy; 9. Free from Hate and Violent Extremism; 10. Strong Enforcement and Real Accountability. Aaronson, 'Data Is a Development Issue'.

rights in third countries [...] which can have a detrimental impact on human rights all over the world".[100] To counter the unchecked export of surveillance technologies, Amnesty International has asserted that the European Union's Dual Use Regulation, related to the use of technologies for both civilian and military application, should be recast and redefined around present and potential digital technology. This should include mechanisms for human rights risks to be flagged and addressed quickly by EU institutions and member states and expanded human rights due diligence with an obligation for exporters to assess the potential domestic and international violations of human rights law and fundamental freedoms in the country of destination.[101]

Nationally, the role of democratic institutions will be paramount. There are legitimate questions around whether the adoption of surveillance technologies in addressing the pandemic runs the risk of eroding civil liberties and whether once introduced they will be difficult to roll back. In many countries, parliament's operations are restricted at the time that they are most needed to scrutinize emergency actions taken, hold government to account and ensure that fundamental rights of citizens are protected. Many parliaments have innovated during the pandemic to maintain functions and should consider how to enhance public engagement and discussion through tools such as online forums and debates. The pandemic provides an opportunity to consider new ways to add "dynamism to institutional oversight and civic participation as cornerstones of good governance".[102]

Democratic institutions also have a key role in enhancing transparency through public engagement and outreach. The introduction of new technologies and the institution of measures during a crisis will earn the trust and acceptance of citizens more strongly if they feel they have a voice. Public trust in science, public authorities and the media empowers the public to do what is right in order to curb the spread of COVID-19 and can mitigate the need to establish surveillance measures that could infringe on civil liberties. In Korea and Taiwan, the building of public trust has been essential to the speed and effectiveness of responses, for example tracing applications are supplemented with extensive testing, transparency of data use and a well-informed public. New technologies introduced and public responses to them have been founded on collaboration, transparency and accountability.[103] The 'demand side' of the issue of surveillance is to increase investments in civic education and digital media literacy.

100 Amnesty International, *Out of Control: Failing EU Laws for Digital Surveillance Export*.

101 *Ibid*.

102 Richard Youngs and Elene Panchulidze, *Global Democracy and COVID-19: Upgrading International Support* (2020).

103 Mark Manantan, 'Agile Governance Crushing COVID-19: Taiwan and South Korea – The Diplomat', *The Atlantic*, 2020, https://thediplomat.com/2020/05/agile-governance-crushing-covid-19-taiwan-and-south-korea/ [accessed 30 August 2020].

European Journal of Law Reform 2020 (22) 4
doi: 10.5553/EJLR/138723702021022004009

II Response at the International Level

At the international level, democracies should collaborate in setting and promoting international norms that protect individual privacy. This can help to set the terms in democratic countries for export of surveillance technologies to the Global South, pushing back against use for repressive purposes.[104] There is also the need for a broad-based discussion at the global level on the principles of the digital economy and something akin to a global digital bill of rights organized by democratic states. Rules that govern data and intellectual property domestically should be translated into international regulatory regimes as they are "the intangible assets on which most of the developed economy, and increasingly the health of our societies, now depend".[105]

In countries in the Global South, data governance should be seen increasingly as a development issue. Countries are already developing rules that govern cross-border data flows as part of regulations on e-commerce and trade agreements can be used to define how and when barriers to data transfers can be put in place.[106] Provision of aid can help develop states in the South's physical and regulatory infrastructure and help promote public digital literacy.[107] This should include demarcating the use of surveillance technologies for legitimate national security purposes from their potential consequences of suppressing human rights.[108]

The international democracy community can help to share lessons about responses in the months ahead. Coordination should involve countries that responded successfully to the crisis and maintained functioning democratic institutions throughout – examples being Canada, Korea, New Zealand and Taiwan – and engage experiences from Asian, African and Latin American democracies. Much can be learnt from the experience of South Korea and Taiwan with digital governance in responding to the pandemic. South Korea has one of the highest densities of surveillance technology yet responded to the crisis with transparency in the use of data, helping to preserve public trust in the authorities.[109] Framing an initiative in these terms would help develop a narrative that presents democracy as helpful in addressing the urgency of responses to COVID-19, combating the notion that there is a trade-off between political freedoms and effective health responses.

104 Nicholas Wright, 'How Artificial Intelligence Will Reshape the Global Order', *Foreign Affairs*, 2018, www.foreignaffairs.com/articles/world/2018-07-10/how-artificial-intelligence-will-reshape-global-order [accessed 30 August 2020].

105 Owen, 'The Case for Platform Governance'.

106 Aaronson, 'Data Is a Development Issue', 1-32.

107 Arora, 'The Bottom of the Data Pyramid: Big Data and the Global South', 19.

108 Wright, 'How Artificial Intelligence Will Reshape the Global Order'.

109 Jung Won Sonn and Jae Kwang Lee, 'The Smart City as Time-Space Cartographer in COVID-19 Control: The South Korean Strategy and Democratic Control of Surveillance Technology', *Eurasian Geography and Economics*, April, 2020.

E Conclusion – Democratizing Use of Surveillance Technologies

The COVID-19 pandemic has the potential to introduce mechanisms of surveillance based on digital technology that are unprecedented. Drones, wristbands, smartphone apps, robotics, microchips, thermal sensors, and other technologies have been employed in the urgency to control the virus, but once introduced they risk altering our "personal habits, affective responses, and day-to-day interactions".[110] COVID-19 could justify a shift to a surveillance culture in many countries, with potential impacts on democracy and culture, politics and economics.

Democratic countries must identify where new powers of surveillance lie in society and where they are originating from and ensure they are exercised in line with human rights obligations, civil liberties and the rule of law. We have witnessed the risks of surveillance in the platform economy to democracy and the way in which it can reverse democratic gains in the Global South. In a fragmented global environment there is now potential for the emergence of a block of countries using surveillance technologies that enhance government control of the public and political opposition that could hasten trends towards autocratization. The response will require an international effort by democracies and supporters of democratic governance. However, inside democracies there should be a national conversation around the type of society that is coming and the ethical use of technologies.

Supporting more informed citizens and civil society is essential in order to improve demand for effective governance of surveillance technologies. In many countries, citizens' groups have mobilized against government responses to the crisis, using government COVID-19 mismanagement "as a wedge to develop renewed engagement on democracy".[111] Well-informed and active citizens in countries of the global North and South are critical to ensuring that surveillance creep does not take place. For example, in Toronto, citizens mobilized to pressure lawmakers to reject the implementation by Google and its parent company, Alphabet, of a 'Sidewalks Lab' project on Toronto's Quayside, turning it into what they called a 'surveillance test bed'.[112] In Kenya, digital rights groups and informed citizens pushed back against a government digital identity programme that would have stored the "fingerprints, eyes, faces, voices, DNA and location of its 50 million citizens".[113] The plan caused alarm about human rights, ethics and privacy breaches among digital advocates and civil libertarians, who demanded the enforcement of data protection. This led to the parliament considering personal data protection laws as the basis for any identity programme.[114] This type of informed citizenry and activism can help to curb repressive uses of

110 Couch, Robinson and Komesaroff, 'COVID-19—Extending Surveillance and the Panopticon'.
111 Youngs and Panchulidze, *Global Democracy and COVID-19: Upgrading International Support*.
112 'BlockSidewalk', www.blocksidewalk.ca/ [accessed 30 August 2020].
113 Aaronson, 'Data Is a Development Issue', 1-32.
114 *Ibid*.

European Journal of Law Reform 2020 (22) 4
doi: 10.5553/EJLR/138723702021022004009

surveillance technologies that risk democratic development in countries in the Global South.

The pandemic has shown that institutions that we depend on are not effective in addressing global challenges and are showing signs of stress. The COVID-19 pandemic has seen many institutions, including parliaments, innovating and opening new avenues for citizen engagement online. This can enable a broader discussion on new methods of public participation and institutional engagement to build trust, foster bottom-up inclusion and pluralism and enhance a rights-based approach to oversight of surveillance measures introduced in democracies.

To help mitigate risks to democracy from surveillance technologies post-COVID, organizations that promote democratic development can consider the following measures:

- Monitoring democratic and civil liberties infringements around use of surveillance technologies during the COVID-19 pandemic;
- Strengthening multilateral initiatives to learn lessons from how democracies have coped with the crisis and how democratic controls of surveillance technologies were put in place;
- Enhancing public understanding of risks of surveillance technologies;
- Supporting democratic civic activism and oversight that is identified by V-Dem as a positive democratic trend and that has emerged during the pandemic;
- Exploring the growth and application in new types of democratic practices that have proliferated under Covid-19.[115]

115 Youngs and Panchulidze, *Global Democracy and COVID-19: Upgrading International Support*.