

GLOBAL CONVERSATIONS

THE DIGITAL FRONTIER

WINTER 2021 ISSUE



EDITORS IN CHIEF

Isabel Jones
David Watson

DIRECTORS OF WRITTEN CONTENT

Alexander Johnson
Matthew Sparling

DIRECTOR OF NEWSWATCH

Erica Wallis

DIRECTORS OF PODCASTS

Anthony Moniuszko
Regina Robbins-Codera

DIRECTOR OF DIGITAL DESIGN

Bethany Fuller

DIRECTOR OF COMMUNICATIONS

Melika Ameresekere

DIGITAL DESIGN ASSOCIATE

Mia Hani

COMMUNICATIONS ASSOCIATE

Melanie Sarmiento-Bravo

ASSOCIATE EDITORS

Desmond Barton
Jared Forman
Samaa Kazerouni
Leanne Lee
Connor Oke
Zachary Spencer
Farley Sweatman

FEATURE CONTRIBUTORS

Sarah A. Jabbar, Yuna Ban, Frédéric Cossette, Amandeep Singh Hanspal, Alexandria Johnston, Reeba Khan, Hilary Lawson, Pierre Miller, Andrea Morales Caceres, Jun Park, Kristen Pearn, Alimah Rehan, Katherine Ross, Joseph Rossi, Rebecca Seward-Langdon, Julia Da Silva, Elliott Simpson, Dorottya Szekely

NEWSWATCH CONTRIBUTORS

Afrah Arif, Imran Bayoumi, Reetinder Chowdhary, Mycala Gill, Madeline Hieman, Azana Hyder, Alexandra Konn, Caitlin Manderville, Pitasanna Shanmugathas, Christian Tramontin

PODCAST CONTRIBUTORS

Luca Bonifacio-Proietto, Larissa Chan, Salwa Hakem, Ella Hartsoe, Sam Hashem, Sky Shi, Paige Smith, Shail Vin

COVER DESIGN BY

Mia Hani

Letter from the Editors in Chief

For those of us fortunate enough to have access to digital technologies, the boundary between the digital and the physical has dissolved. Digital technologies take centre stage in our lives as many of us work remotely, connect with friends and family online, and turn to streaming services, e-books, online games, and more to relax.

However, the increasing presence of digital technologies extends far beyond our personal spheres. The past year has seen the rampant proliferation of disinformation-based conspiracy theories on social media platforms and fringe news sites, culminating in the January 6 attack on the U.S. Capitol. The exacerbation of the digital divide—the gap between those with access to internet and communications technologies and those without—has laid bare the stark inequality that characterizes many societies worldwide. Developments in the virtual sphere are having real world political, social, and economic consequences.

While it's tempting to think of the internet and other virtual spaces as separate from our physical realities, recent developments prove that the digital and the physical are inextricably linked. Technological solutions continue to be favored to solve the world's increasingly complex problems, yet their rapid proliferation gives us cause for concern. The states, corporations, and individuals that control the "digital frontier" will be able to exercise power far beyond its bounds. Questions of who is granted access to digital developments, how they are regulated, and which associated behaviours and norms prevail will be key in determining the future of our global society.

For the Winter 2021 issue of Global Conversations, we challenged our writers to consider the implications of this digital frontier for their respective areas of focus. We commend our writers and editors for their diligent analyses of the consequences and opportunities presented by our increasingly digitized realities in this exceptional issue.

Editors in Chief,

Isabel Jones & David Watson

Introduction

The digital frontier represents a new chapter for humanity. Enabled by a series of extraordinary technological developments, it constitutes society's greatest response to disruptive change. The growing accessibility of digital technologies has allowed many to create opportunities that transcend geography, industries, and cultural barriers. An ecosystem of unparalleled utility, the digital frontier is the product of technological evolution that has been gaining momentum for centuries. Although much of this progress has been driven by humanity's proclivity for innovation, events like the COVID-19 pandemic demonstrate that nature can also catalyze momentous technological changes to the way we work, learn, and live.

The confluence of our physical and digital worlds carries with it enormous potential for both progress and peril. Cryptocurrencies can offer viable alternatives for those oppressed by unfair or broken financial systems. Social media has given a voice to people fighting oppression globally. Digital vaccine passports promise a safer transition to a post-COVID-19 era at the cost of privacy risks and other ethical concerns. The digital frontier has also permitted disinformation, suppression, hate, and violence to thrive, leaving the global community subject to the whims of large multinational corporations who decide how to police their own platforms.

The global scale of this rapid transformation is forcing us to reevaluate how digital development occurs and the ways in which humanity may be at risk. For the Winter 2021 issue, we asked our writers to reflect on some of the opportunities and challenges presented by the rapid evolution of the digital frontier. We hope their insights will encourage you to consider how digital technologies can be used inclusively to propel our world forward.

*Directors of Written Content,
Alexander Johnson & Matthew Sparling*

t h e d i g i t a l f r o n t i e r

8 Nunavut's Connectivity Gap Signals an Opportunity for China in the Arctic

BY HILARY LAWSON | INDIGENOUS AFFAIRS 8

11 Using Tech to Control the Pandemic: How Canada Can Learn from Taiwan and South Korea

BY YUNA BAN | ASIA-PACIFIC AFFAIRS 11

14 How Canada Can Revamp its Digital Infrastructure for a Post-COVID-19 World

BY ELLIOTT SIMPSON | CANADA IN THE WORLD 14

17 Education and the Digital Divide in Latin America: The Impact of COVID-19

BY ANDREA MORALES CACERES | SOUTH & CENTRAL AMERICAN AFFAIRS 17

20 Where Will Digital Education Take the SWANA Region?

BY SARA A. JABBAR | SWANA AFFAIRS 20

23 Identification, Please: The Benefits and Risks of Digital Vaccine Passports

BY DOROTTYA SZEKELY | MIGRATION 23

26 Digital Authoritarianism: How Regimes Track and Silence Dissidents Across the Globe

BY JOSEPH ROSSI | HUMAN RIGHTS 26

29 Social Media's Role in Political and Social Movements in Africa

BY REBECCA SEWARD-LANGDON | SUB-SAHARAN AFRICA 29

32 Search Engines and the Power They Hold: Google's Role in Perpetuating Hate Speech, Racism, and Sexism Online

BY KATHERINE ROSS | TECHNOLOGY AND INNOVATION 32

35 How Pandemic Lockdowns Enabled the Weaponization of the Internet Against Women

BY JULIA DA SILVA | GENDER AND IDENTITY POLITICS 35

37 Digital Disease: Understanding the Online Spread of Anti-Vaccination Sentiment

BY ALEXANDREA JOHNSTON | GLOBAL HEALTH 37

39 How Social Media Became the Digital Battleground in the Fight for American Democracy

BY KRISTEN PEARN | NORTH AMERICAN AFFAIRS 39

42 Europe Confronts Tech Giants Over Consumer Protection and Content Moderation

BY PIERRE MILLER | EUROPEAN AFFAIRS 42

45 True or False: Is It Time for International Law to Address Disinformation?

BY FREDERIC COSSETTE | INTERNATIONAL LAW 45

48 Uber Great, or Great for Uber? Understanding the Future of an Economy Without Employees

BY ALIMAH REHAN | INTERNATIONAL TRADE AND BUSINESS 48

51 Technology Alone Cannot Fix Climate Change

BY REEBA KHAN | ENVIRONMENT AND CLIMATE CHANGE 51

54 A New Way Forward? The Cryptocurrency Revolution in Developing Countries

BY JUN PARK | GLOBAL DEVELOPMENT 54

Nunavut's Connectivity Gap Signals an Opportunity for China in the Arctic

BY HILARY LAWSON | INDIGENOUS AFFAIRS



When Mumilaaq Qaqqaq, the member of Parliament for Nunavut, needs to participate in virtual sittings of Parliament, she has to join them from her apartment in Ottawa. Slow internet connectivity in the territory means that videoconferencing is next to impossible. Nunavut is served by a broadband satellite network, but inclement weather can make the satellite connection unpredictable. Some days, the internet connection in her constituency office in Iqaluit is so slow that she is unable to send emails.

The COVID-19 pandemic has exposed a glaring connectivity gap in Canada. Nunavut is the only province or territory that relies entirely on satellite internet, which is slow, unreliable, and expensive. The fastest possible speed in Nunavut is 15 megabits per second, eight times slower than the Canadian average. Beyond that, Nunavut's telecommunications service providers offer no option

for unlimited usage. It would cost an Inuit household in Nunavut at least \$7,000 yearly to reach the level of data usage enjoyed by the average Canadian household.

The fastest possible speed in Nunavut is 15 megabits per second, eight times slower than the Canadian average.

The connectivity gap in Nunavut is not new, but the pandemic has made its effects more acute. As workplaces and

schools move their activities online, Nunavut residents who need to join a lecture or meeting by video are forced to pay prohibitive overage charges or simply forego participation. A bad connection also makes it challenging to access online health services, public health information, and up-to-date news about the pandemic.

A BARRIER TO SELF-DETERMINATION

A report commissioned by Nunavut Tunngavik Inc. found that fixing Nunavut's infrastructure deficit is crucial to Inuit self-determination. Poor broadband infrastructure is deeply interconnected with other economic challenges and is a major barrier to economic and educational opportunities. Canada's colonial legacy and continued under-investment in the Arctic have left communities in the North with negligible access to essential services. As a consequence, some Inuit are forced to leave the territory to access healthcare, find work, or attend school. Travelling south is expensive and can isolate Inuit from friends, family, and community support. And so, as the COVID-19 pandemic shifts work, education, socializing, and organizing online, those who lack good, affordable internet service will find it harder to participate in the new digital world.

Better internet access could amplify other efforts to improve wellbeing in the territory. Inuit in Nunavut live in 25 separate communities, all of which are accessible only by plane. The physical distances between these communities are vast. Online banking, for example, offers a solution for Nunavut Inuit whose nearest bank branch is hundreds of kilometres away. Improved connectivity could also increase access to telehealth services and online counselling, which could save lives in a territory grappling with a devastating suicide crisis. Instead, Nunavut residents must travel long distances for opportunities or services that could otherwise be delivered digitally. In MP Qaqqaq's case, she is unable to represent her constituents in the virtual House of Commons without travelling thousands of miles south just to secure a more reliable internet connection.

THE HUAWEI CONNECTION

While the reliability of satellite broadband is improving,

it is still subject to signal interference and cannot match the speeds of fibre-based broadband. And because of the territory's remoteness and small population, the cost of infrastructure spending is high. However, there are currently several proposals to bring a terrestrial fibre-optic connection to Nunavut. One of these is the Iqaluit and Kimmirut Fibre-Optic Link proposed by the Government of Nunavut, which was originally slated to connect Iqaluit by marine cable to an existing network in Nuuk, Greenland. The Nuuk line, called Greenland Connect, was outfitted with new equipment in 2017 by Huawei Marine, a subsidiary of the Chinese telecommunications company Huawei.

There is growing concern among some Canadian policymakers and maritime security scholars that China's increased economic activity in the Arctic could threaten Canadian sovereignty.

China has emerged as a major player in the Canadian Arctic. Chinese companies continue to expand infrastructure investments and marine shipping in the region. The melting of the Arctic sea ice, hastened by climate change, has created opportunities for resource exploration, though extractive projects risk disturbing the already-fragile Arctic ecosystem. Huawei Canada has committed to connecting 70 rural and remote communities to high-speed broadband in Canada's North by 2025. But Huawei has been a flashpoint in Canadian-Chinese relations since the detention of its CFO Meng Wanzhou in 2018, and the company's stake in the Greenland Connect line complicates this project for Nunavut.

There is growing concern among some Canadian poli-

PHOTO SOURCE: FLICKR, LESLIE PHILIPP

cymakers and maritime security scholars that China's increased economic activity in the Arctic could threaten Canadian sovereignty. Indeed, China has developed a reputation for territorial assertiveness over matters of business. Chinese leadership has already signaled its intent to establish a permanent shipping route through the Northwest Passage, which Canada considers to be internal waters.

But for some Nunavut Inuit, it matters little that prospective investors in Arctic infrastructure are Chinese rather than Canadian. Since colonization, the Canadian government has relied on Inuit presence in the Arctic as a means to assert its sovereignty, while systematically under-servicing their communities, forcibly relocating their homes, and putting Inuit children in residential schools. As a result, the infrastructure gap between Nunavut and the rest of Canada persists. Chinese companies like Huawei that offer sustained investment in much-needed infrastructure are filling the gap left by the Canadian government, which has not moved quickly enough to meet the immediate needs of Nunavut Inuit. That is why some view China's economic ambitions in the Arctic as an alternative way for Nunavut to gain more agency over its economic future.

Still, in January, the Government of Nunavut announced that it would terminate its original plan to link Iqaluit to the Greenland Connect line. Instead, a new line will run south, eventually connecting with the North American fibre-optic backbone in Montreal. A spokesperson for the Government of Nunavut told Nunatsiaq News that the territorial government is now working with the federal government to develop an official policy on Huawei. Meanwhile, a new company called CanArctic Inuit Networks has proposed a separate fibre-optic line from Iqaluit to Newfoundland. Better Internet is coming to Nunavut—but until then, its residents will have to contend with satellites.



Hilary Lawson is a first-year student in the Master of Global Affairs program at the Munk School of Global Affairs & Public Policy. She worked for 5 years as a political staffer on Parliament Hill, first for a Member of Parliament and then as an advisor to the Minister of Indigenous Services.

Her research interests include information warfare, surveillance and privacy rights, Indigenous self-determination, and criminal justice transformation. She holds a bachelor's degree in Conflict Studies and Human Rights from the University of Ottawa.

Using Tech to Control the Pandemic: How Canada Can Learn from Taiwan and South Korea

BY YUNA BAN | ASIA-PACIFIC AFFAIRS



ALTHOUGH the COVID-19 pandemic began in Wuhan, the capital of Hubei province in China, it rapidly spread to neighbouring countries, including Taiwan and South Korea. Equipped with previous pandemic experience from SARS in 2003 and MERS in 2015, the governments of Taiwan and South Korea did not hold back in leveraging their pre-existing technology to track the spread of the virus and “flatten the curve.” This digital infrastructure was government-led, and was used to track individuals’ infection status, movements, and contacts. Citizens of Taiwan and South Korea also complemented their digital infrastructure’s effectiveness by promptly wearing masks and adhering to social distancing in public spaces. In Canada, the idea of actively using technology to collect data has raised serious concerns among the public regarding data privacy and individual rights. The absence of a collectivist attitude in civil society and the lack of government-led digital infrastructure has made it difficult for the Canadian government to respond to the pandemic as effectively as several East Asian governments.

PHOTO SOURCE: FLICKR, WANG YU CHIN

HOW TAIWAN GOT IT RIGHT

Both Taiwan and South Korea’s governments recognized that their COVID-19 outbreaks stemmed from flows of international travel and thus used technology to closely track travellers, even before they entered the country. Taiwan’s emergency Central Epidemic Command Control cooperated with the National Communications Commission to create a cohesive strategy using a myriad of platforms, including broadcast media, memes, YouTube, and even animated online stickers depicting the Minister of Health and Welfare, Chen Shih-chung. As the government with the most successful emergency strategy, the Taiwanese government was the first to implement systematic mobile phone tracking to enforce and monitor mandatory quarantines. The closely managed and subsidized 14-day quarantine has resulted in Taiwan recording less than 1,000 cumulative confirmed cases as of February 3, 2021. This quarantine system provides each individual with a designated QR code to track GPS locations

upon arrival. If the GPS location does not match with the registered address or if travellers do not respond to messages, police officers will check to see whether quarantine requirements are being breached.

Both South Korea's public and private sectors use its developed technology and digital infrastructure to track COVID-19.

Canada requires that all travellers entering the country must submit their quarantine plan using the “Arrive-CAN” app prior to boarding their flight. Importantly, it specifies that the app does not use GPS to track individuals’ locations. Unlike the Taiwanese government, the Canadian government reflects Western individualist ideology by emphasizing privacy protection on multiple government websites, recognizing Canadians’ concerns over the infringement of their privacy rights. In contrast, the Taiwanese population tends to believe that individual sacrifices are needed to protect their community. Quarantine upon arrival is also flexible in Canada, where public health workers barely call people in quarantine and only require a simple online symptoms check. In South Korea, workers from local public health centres make calls to individuals in quarantine every day to ask for their exact temperature. Although Canada is slowly learning from other effective quarantine models, it continues to receive criticism for both its management of public health and its protection of individual rights.

Another interesting digital infrastructure in Taiwan was developed through cooperation between the Taiwanese government and the country’s civil society groups. The “g0v” community is a group of civil activists and hackers that aim to “use technology for the public good.” Amid the pandemic, g0v designed a platform to improve the transparency of information related to the pandemic. For example, with the help of Taiwanese Digital Minister

Audrey Tang, g0v created a “mask map” reporting the quantity of available masks in each pharmacy. Initially, the Taiwanese government prevented mask shortages by implementing the “Mask Real-Name System” to impose a limit of nine masks for each person during a two week period. The mask map provided additional information on mask availability to allow Taiwanese people to purchase masks more easily, avoiding the early mask and sanitizer shortages seen in Western countries. More websites that provide visualized data have since been developed to provide transparent information on COVID-19-related supply logistics. Taiwan’s innovative pandemic-fighting websites and apps were made possible due to data provided by the government. However, it would likely be a challenge to implement similar tools in Canada due to privacy concerns.

SOUTH KOREA’S SUCCESS

South Korea has almost one and a half times the population of Canada but only one tenth the cumulative number of confirmed cases. The Korea Disease Control and Prevention Agency involves an Office of Communication that was designed to “perform communication in the emergence of infectious diseases.” Long before COVID-19 started to spread in South Korea, the Office of Communication possessed the necessary capacity to send out text messages through a number of channels, including its “secure emergency text message system.”

Both South Korea’s public and private sectors use its developed technology and digital infrastructure to track COVID-19. South Koreans receive emergency text messages from the government throughout the day if their city has had an outbreak. In addition, in cases where there is potential for interaction with an infected individual, text messages are sent out indicating the time and the exact location of the infected person throughout the day. This information could also be used to encourage people who may have been exposed to get a COVID-19 test. In addition, “Corona 100m” was developed by individuals in Korea’s private sector who thought the government’s method was not efficient enough. The app sends a notification warning when the user comes within 100 meters of a location that has recently been visited by an infected individual. Other corporations have built similar COVID-19 tracking apps in order to help flatten the curve.

LESSONS FOR CANADA

In Canada, the government launched the “COVID Alert” app in late July. It took six months for 16 per cent of the Canadian population to download it; “Corona 100m” was downloaded by seven per cent of the Korean population in one month. Most notably, unlike South Korean apps, the Canadian government has emphasized the primacy of personal data protection, claiming that COVID Alert does not use GPS or track location. The app is also unavailable in Alberta and British Columbia, provinces that rank third and fourth for the highest number of confirmed COVID-19 cases in Canada. This comparison of COVID-19 apps from two countries demonstrates the extent to which individualism and user privacy have limited the extent of Canada’s digital fight against COVID-19.

This comparison of COVID-19 apps from two countries demonstrates the extent to which individualism and user privacy have limited the extent of Canada’s digital fight against COVID-19.

Solid digital infrastructure is the foundation upon which Taiwan and South Korea have built their successful responses to the pandemic. This was possible due to effective communication systems which were supported by collective action and significant budgetary commitments from their respective governments. For both East Asian governments, their emergency response infrastructure, public health systems, and their societies’ widespread adoption of data transparency formed a multi-pronged approach that has been effective in combatting the pan-

dem. The tension between Western liberal values and data transparency in Canada’s pandemic response has complicated the government’s efforts to adopt a quarantine system that uses digital infrastructure to flatten the curve. The Canadian government should consider the strategies used by these East-Asian democracies in order to identify a middle ground that satisfies both public health and individualistic concerns in its own response to the pandemic.



Yuna Ban is a first-year Master of Global Affairs student also pursuing a Collaborative Master’s Specialization in Contemporary East and Southeast Asian Studies. She graduated from the University of Toronto with an Honours Bachelor’s

of Arts studying International Relations, Political Science, and History. Prior to joining Munk, she worked at the Consulate General of the Republic of Korea in Toronto. Her previous experience with the AAS-in-Asia 2017 Conference, Canadian Centre for the Responsibility to Protect, and research assistant work prompted her academic focus in innovation policy. Upon graduation, Yuna aspires to use her quantitative analytical skills to contribute to the international studies of the Asia-Pacific.

How Canada Can Revamp its Digital Infrastructure for a Post-COVID-19 World

BY ELLIOTT SIMPSON | CANADA IN THE WORLD



ON May 1, 2020, the C.D Howe Institute officially declared what most Canadians already knew: that Canada was in a recession caused by the COVID-19 pandemic. In April of 2020 alone, two million Canadians, including this contributor, lost their jobs entirely and many more had their hours reduced. While the Canadian economy showed some resilience over the summer months as public health restrictions eased, caseloads shot back up at the end of 2020. Some of the economic rebound was wiped out as unemployment hit 8.6 per cent and the economy lost another 63,000 jobs in December, the first month of net job loss since April, when the recession was first announced.

PUBLIC INFRASTRUCTURE

Throughout modern economic history, public spending on infrastructure has often been used as a powerful tool by a government trying to pull its economy out of a recession or depression. Perhaps the most famous example

...unemployment hit 8.6 per cent and the economy lost another 63,000 jobs in December, the first month of net job loss since April, when the recession was first announced.

of this is President Roosevelt's New Deal that saw a mas-

PHOTO SOURCE: UNSPLASH, ARI HE

sive amount of public spending on federally funded infrastructure projects as a means to combat the Great Depression. Canadians need not look beyond their borders for such an example, however. In the post-war years when Canada's economy seemed stagnant, investment in public infrastructure was used to great effect, the most visible result of which was the Trans-Canada Highway that connected Canadians from coast to coast. More recently, the Conference Board of Canada estimated that nearly a quarter of all growth in productivity in Canada in recent years is the result of public infrastructure investment. Taking a longer view, Statistics Canada estimates that up to half of all productivity growth between 1962-2006 can be attributed to investment in public infrastructure.

Traditionally used to refer to roads, bridges, and gas lines, the definition of public infrastructure has extended in the 21st century to include the all-important digital services we rely on every day in our personal and professional lives.

The challenges of deploying infrastructure across Canada are similar, be it a highway or a cell tower. Canada is vast, and there remains an unacceptable gap in access to broadband services. Indigenous communities have been left behind. Over two thirds of on-reserve homes do not have access to high-speed internet, and students on reserves in Northern Ontario have had to resort to using fax machines during COVID-19. This is keenly felt in the far North—the Canadian Radio-television and Telecommunications Commission (CRTC) reported that fewer than half of Nunavut households have download speeds of 5Mbps, well shy of government targets.

THE KEY TO CANADA'S FUTURE SUCCESS: 5G

Even considering this, however, Canadians on average enjoy the third fastest mobile download speed globally according to a report by BCG's Centre for Canada's Future. Also, a stable regulatory environment has contributed to Canada outpacing global peers on digital infrastructure investment, while telecom investment per capita in Canada sits at \$255 CAD versus the OECD average of \$156 CAD.

Despite the unequal access to broadband across the country, Canada has, up until now, done very well compared to its peers in the broader project of building the digital infrastructure needed for consumers, the tech industry,

and businesses in general to function. However, whether it will be able to replicate that success in rolling out the next generation of connectivity, namely 5G, remains to be seen.

The challenges of deploying infrastructure across Canada are similar, be it a highway or a cell tower.

5G represents the next digital infrastructure challenge that will define and enable Canadian economic competitiveness in the next century. Providing never-before-seen network agility, and with speeds up to 20 times faster than existing 4G infrastructure, 5G networks are critical to Canadians being able to participate in the next wave of human innovation. While 3G and 4G was defined largely by faster connections—an improvement on what already existed—5G represents so much more, especially to business consumers.

5G allows for the technology that will define the 21st century and beyond. The stuff of science fiction, including autonomous vehicles, virtual reality, IoT (internet of things), drones, and even previously unthinkable remote surgery, will lean on 5G networks rooted in digital infrastructure to grow and thrive in Canada.

The tech industry accounted for 4.7 per cent of the Canadian economy in 2019, and net tech employment in Canada hit 1.72 million workers. Also, jobs in tech tend to outpace the average Canadian salary by about 52 per cent. Despite COVID-19 (and in some cases thanks to COVID-19), the Canadian tech industry is increasingly important to Canada's competitiveness and economic health. At the present moment it is on solid footing, according to the Cyberprovinces 2020 report by CompTIA, an industry association. This same report notes a growth in job postings in areas such as IoT, blockchain, and augmented and virtual reality—all of which will soon need to rely on 5G to survive.

Canada is already lagging behind countries such as the United States, South Korea, and the United Kingdom in 5G rollout. The confusion surrounding the “Huawei Problem” notwithstanding, there has been a lack of clarity from Ottawa regarding Canada’s strategy in deploying 5G technology.

PREPARING FOR A POST-PANDEMIC WORLD

Beyond the tech industry, existing wireless and broadband networks supported by nationwide digital infrastructure have been able to handle the 40 per cent surge in traffic caused by COVID-19. Policymakers would do well to recognize that this growing reliance on digital networks will persist after COVID-19. If Canada’s economy is to grow and thrive, Canada cannot miss this critical opportunity to reinvest in digital infrastructure and deploy 5G technology.

Canada is already lagging behind countries such as the United States, South Korea, and the United Kingdom in 5G rollout.

Based on current projections, Canada’s federal government is set to add \$1 trillion CAD to Canada’s debt between the end of 2019 and the mid 2020’s, and according to the Fraser Institute, combined federal and provincial debt now equals 91.6% of the economy. Canada is in a perilous economic situation. While the vast amount spent so far on helping the nation recover from COVID-19 is certainly warranted, government spending is not a substitute for growth in the long run.

Whereas Germany has its 2030 Industrial Strategy and the United States is putting R&D at the forefront of economic recovery, Canada does not (yet) have a plan. The country should learn from this pandemic, and place a big

bet on the digital infrastructure that will allow Canadian businesses and consumers to roar out of this pandemic and into the 2020’s.



Elliott Simpson is a first-year student at the Munk School of Global Affairs & Public Policy at the University of Toronto. He graduated from the University of Edinburgh in 2016. Then worked with Deloitte Canada’s Public Sector Transformation Team. In 2019, Elliott joined the team at Ritual and launched the app in Montreal. He has worked in several industries including telecommunications and marketing, and spent some time consulting within the Scottish Parliament. Elliott’s interests lie mostly in the sphere of global security, and defence – and he has been conditionally accepted to the Royal Canadian Navy reserve unit at HMCS York.

Education and the Digital Divide in Latin America: The Impact of COVID-19

BY ANDREA MORALES CACERES | SOUTH & CENTRAL AMERICAN AFFAIRS



AFTER the World Health Organization (WHO) declared COVID-19 a global pandemic in March 2020, schools around the world began to suspend face-to-face learning and abruptly transitioned to distance learning strategies. According to the Inter-American Development Bank, the pandemic has disrupted the education systems of approximately 1.6 billion learners in over 190 countries. In addition to the health and economic challenges that COVID-19 has presented in the past year, the impact on education has been one of the most prominent effects of the pandemic. Students from Latin America and the Caribbean (LAC) are no exception, with estimates stating that children in the region lost 174 days of learning last year and remain at risk of losing more in the upcoming school year.

While most studies show that children are not as susceptible to contracting COVID-19 in comparison to older populations, the pandemic has still greatly impacted their lives through the disruption of their education and

learning experiences. With almost every country in the LAC region suspending face-to-face classes by the end of March 2020, more than 165 million students across different levels of education found their learning routines suddenly disrupted. In an effort to mitigate the negative consequences of COVID-19 on education, countries in the region began to roll out a variety of initiatives to support remote learning, including implementing internet-based forms of learning and broadcasting educational programmes through media outlets. Ecuador, for instance, used radio broadcasts and television programs to reach poor communities in cities and young students in rural areas who lacked access to a reliable internet connection. A few countries have provided additional online resources to support students’ transition to online learning. El Salvador’s Ministry of Education offers a website with educational resources separated by grade and a call centre which can be reached via email or WhatsApp for students and parents in need of support. Despite these rapid attempts to support student learning, existing in-

PHOTO SOURCE: UNSPLASH, FELIPE SCHIAROLLI

equalities in accessing digital technologies in the region have left certain students behind while others are only slightly affected, thus widening education gaps in the region.

Ecuador, for instance, used radio broadcasts and television programs to reach poor communities in cities and young students in rural areas who lacked access to a reliable internet connection.

THE DIGITAL DIVIDE IN LATIN AMERICAN EDUCATION

With most countries in the region now relying on online delivery methods to provide education, the past year has revealed the depths of online educational inaccessibility. In LAC countries, approximately one third of the population has no internet access. However, this figure paints a misleading picture. In 2019, for instance, more than 80% of Chileans had internet access, compared to less than 30% of Nicaraguans. Disparities in internet access are not only felt between countries, but also within countries, where rural populations are less likely to have internet than urban populations. To illustrate this, a national opinion survey in Bolivia found that 42 per cent of the population reported having access to a computer and 10 per cent had access to a permanent internet connection. When considering solely rural populations, access to a computer dropped to 18 per cent, while permanent internet connectivity dropped to a low of 3 per cent. The lack of internet and computer access in Bolivia's rural areas led the country's interim government to cancel the

school year in August 2020. With a typical school year in Bolivia starting in February, this meant that students only received one month of regular in-person schooling before the transition to online learning—for those able to access it—began in March. Consequently, students without reliable internet access have been severely deprived of quality learning for over a year.

In addition to the rural-urban divide, the socioeconomic differences between households mean that certain students have better access to online learning resources at home such as laptops, reliable internet, and mobile phones. Based on their geography and socio-economic status, these students also have access to educational institutions that are better equipped for the shift to online learning. A joint ECLAC-UNSECO report found that in the seven LAC countries studied, between 70 to 80 per cent of students in the highest socioeconomic quartiles have a laptop at home, while the same was only true for 10 to 20 per cent of students in the lowest socioeconomic quartile. This figure raises questions as to which children have been able to access online schooling and how lacking laptop access has impacted online attendance and learning outcomes in the previous school year. Notably, Uruguay and Chile were exceptions to this, as the report attributes their greater electronic accessibility to programmes that made public devices available prior to COVID-19. This demonstrates the value provided by funding and investing in programs that prioritized internet access in the region ahead of the current crisis.

Furthermore, the divide in respect to educational resources is further widened between public and private schools. A UNICEF report estimated that three out of four children from private schools had access to quality distance learning at home in the previous academic year, compared to one out of two children in public schools. This difference in ratio reinforces socio-economic divides which extend notable differences between the availability and accessibility of online classes and recordings in public school settings compared to private school settings.

It is important to note that the effects of the digital divide in education have also had secondary impacts on other aspects of student physical and mental well-being. Closures have affected students' access to school meal programs, in addition to mental health services and recreational activities. Thus, not only has student learning been severely impacted by online schooling, but children may also face

nutritional and mental health repercussions. The limited access to essential resources puts an additional economic and emotional burden on students who normally relied on school-provided support programs. Moreover, the consequences of online school have also taken physical and mental tolls on teachers. In addition to the difficult task of maintaining regular teacher-student relationships online, educational staff have also been faced with the exhausting challenge of providing emotional support to students and their families during the pandemic.

The vast majority of schools in the Southern Hemisphere begin their school years in February or March, meaning these countries are now at a critical juncture.

MOVING FORWARD

Intergovernmental organizations have stated that the effects of the COVID-19 pandemic on education will only exacerbate existing inequalities in the Latin American region, both between and within countries. These organizations predict that the region's educational strides from the past two decades risk being lost in the coming years as dropout and enrollment rates are affected by online learning. UNICEF has called the effects of COVID-19 on children's schooling a "generational catastrophe," predicting that the school enrollment of first-time students could decrease by almost two per cent and that three million children might never return to school worldwide.

The vast majority of schools in the Southern Hemisphere begin their school years in February or March, meaning these countries are now at a critical juncture. Whether this new school year will signal the continued widening

of the educational gap or an opportunity to address the region's digital divide remains to be seen. Although many governments in the LAC region have demonstrated their commitment to address challenges within online education, government leaders must learn from their experiences in 2020 to evaluate the effectiveness of online learning initiatives. This monitoring and evaluation process will ensure that governments are able to identify gaps in the programs and support children who are at risk of being left behind in the upcoming school year. The path forward must prioritize access to an education system that is sustainable and inclusive.



◇

Andrea is a second-year Master of Global Affairs candidate at the Munk School of Global Affairs & Public Policy. She graduated in 2019 from Wilfrid Laurier University with a combined Honours Bachelor of Arts in Global Studies and French in addition to a Spanish minor. Over the summer, she interned at the International Organization for Migration (IOM) in their Integration and Migrant Training (IMT) Unit. Her current research interests include international development, gender equity, and forced migration, specifically in the Latin American region.

Where Will Digital Education Take the SWANA Region?

BY SARA A. JABBAR | SWANA AFFAIRS

Note: In this issue, we will represent the region as Southwest Asia and North Africa (SWANA) rather than the Middle East and North Africa (MENA), due to the latter's colonial connotations.



COVID-19 has disrupted education in the Southwest Asia and North Africa (SWANA) region, threatening the area's long-term economic future. The risk is particularly pressing as those under 25 form up to 60 per cent of the Arab world's total population of over 420 million. According to a UNICEF report, COVID-19 has forced 110 million children out of schools in the SWANA region alone.

However, local governments quickly adopted digital learning platforms to mitigate the risks of school closures. For example, Jordan developed a platform called Kolibri which delivers open educational resources and is available

for offline and online use. Other countries such as Egypt are using multi-modal approaches to reach young people, employing radio, television, and print tools in addition to the internet. Although the challenges it poses are enormous, the shift to digital platforms might also present an opportunity for the region to prepare for future disruptions to education.

LONG-TERM IMPLICATIONS OF STAGNATION

The risks of disrupted education are severe, especially giv-

en the SWANA region's volatile political, economic, and security climates. The lack of education contributes to a harsh cycle: women and girls already face higher barriers to education, leading to increased gender inequality, and under-educated youth are less likely to be employed, leading to poverty. Poverty is in turn a contributing factor to violence. Heightened conflict displaces more people, causing more disruption to education, and the cycle continues. Additionally, under-educated young people are at a higher risk for recruitment by extremist groups such as Daesh (ISIS). Likewise, prolonged interruptions to education could delay the region's achievement of the UN's Sustainable Development Goals, as the reduction of financial inequality, promotion of gender equality, and fostering of innovation are closely tied to education.

The risks of disrupted education are severe, especially given the SWANA region's volatile political, economic, and security climates. The lack of education contributes to a harsh cycle...

The risks are particularly severe for the most vulnerable group in the region—refugees. The move towards e-learning often excludes them due to a series of compounding variables, including a lack of internet access, poverty, and overcrowded living conditions. Syrian refugees in Jordan already endure poor standards of living, such as a lack of running water and insufficient housing. Barriers to education, such as a lack of internet access, make it much more difficult to escape from these situations. As stated by Judith Finnemore, an education consultant based in

the United Arab Emirates, “education is the only route out of continued poverty for refugee children.”

INTERRUPTED EDUCATION: COMMON TO THE REGION

Unfortunately, disruptions to education are not new for thousands of families across the SWANA region. A study by the Dubai School of Government found that almost 35 per cent of respondents reported disruptions to their child's education on several occasions in the past two years, and 7 per cent reported that their child's education was interrupted on multiple occasions for long periods.

These interruptions suggest a desperate need for educators and policymakers to design new solutions that provide a stable learning environment, especially with the prevalence of conflict in the region. In the digital age, there are unparalleled opportunities to invest in human capital through education, catch up to the educational standards of the rest of the world, and give young people in the SWANA region a head-start on their future careers.

COVID-19: AN OPPORTUNITY?

Although the virus itself poses a serious risk, the COVID-19 crisis may have provided the necessary push to address the long-standing instability in the regional education system. E-learning offers ministries of education across the region a chance to restructure failing educational systems. Many do not have the physical capacity to serve all the community's children, and the region lacks high-quality education centres.

The SWANA region's young people argue that the education they receive does not provide them the skills they need to succeed in competitive global markets. These include critical thinking, problem-solving, and communication skills. Since the region is home to some of the highest youth unemployment rates in the world, leaders must prioritize developing educational institutions. Virtual learning could improve collaboration between educators of all disciplines and provide students more subject choices, as educators would not be limited by their physical locations.

However, the multiple shortcomings of e-learning need

PHOTO SOURCE: FLICKR, WORLD BANK PHOTO COLLECTION

to be addressed. These include the need to train educators to use new platforms, the potential lack of infrastructure, the risks of minimal participation and easy distraction, and the reality that everyone does not have access to the same resources. A UNESCWA report found that just over half of households in the SWANA region have internet access. This excludes many from accessing the potential benefits provided by the shift to virtual learning.

Since the region is home to some of the highest youth unemployment rates in the world, leaders must prioritize developing educational institutions.



◇

Sara A. Jabbar is a first-year student in the Master of Global Affairs program with an emphasis on security. As a product of her background and upbringing, she has always been interested in politics and history so she co-founded a project with her sister, @shabab12.9, to discuss these subjects. Shabab12.9 focuses on producing graphics and sharing research on politics, history, mental health, climate justice, freedom of movement (among other topics) particularly as they relate to the SWANA region. In June 2019, she completed her undergraduate degree in Business Administration at UofT. Since graduation, she has completed a Big Data Analytics certification at York University. She is also passionate about holistic healing techniques and wellbeing practices.

shabab12.9, to discuss these subjects. Shabab12.9 focuses on producing graphics and sharing research on politics, history, mental health, climate justice, freedom of movement (among other topics) particularly as they relate to the SWANA region. In June 2019, she completed her undergraduate degree in Business Administration at UofT. Since graduation, she has completed a Big Data Analytics certification at York University. She is also passionate about holistic healing techniques and wellbeing practices.

MOVING FORWARD

SWANA leaders need to realize that disrupted education harms their young people in the long-term and limits the development of the region as a whole. It increases the likelihood of dropping out, and increases the risks of continued poverty, unemployment, and violence. The region must prioritize investing in its human capital.

Through major disruption, the COVID-19 pandemic has shown the SWANA region that it has the opportunity to use e-learning technologies to bridge the educational gap between the region's youth and the global average and address the chronic disruptions endemic to the region. The digital transformation offers policymakers the chance to create a blended e-learning model that prepares the region's youth to excel in an ever-changing labour market. The success of these policies will not only be measured by how well the region navigates the COVID-19 pandemic, but how well the region prepares its educational systems for the post-pandemic world.

Identification, Please: The Benefits and Risks of Digital Vaccine Passports

BY DOROTTYA SZEKELY | MIGRATION



WHILE the COVID-19 pandemic is far from over, the development and deployment of vaccines remains a remarkable and celebrated achievement. While governments around the world are racing to vaccinate their populations, insufficient vaccine supplies have impeded success for many countries. As of January 2021, more than 50 countries had administered 94,000,000 doses, equal to 1.2 doses for every 100 people in the world. Most doses have been reserved for priority groups, including front-line healthcare workers, the elderly, and those who are especially vulnerable.

Global vaccine deployment has not been evenly distributed, and vaccination efforts have yet to start in Africa. As a result, lower income countries are relying on COVAX, a global initiative which guarantees fair and equitable access to COVID-19 vaccines to every country in the world. Despite initiatives like COVAX, many vulnerable

groups remain overlooked. To date, out of 90 countries currently developing national COVID-19 vaccination strategies, only 51 to 57 per cent have included refugees in their plans. As long as large populations of marginalized groups are left out of vaccine distribution plans, the herd immunity needed to control the transmission of the virus worldwide will remain out of reach. Vaccinating these populations is fraught with challenges, as refugees especially are concentrated in lower-income countries that simply lack the infrastructure and resources necessary to implement comprehensive vaccine rollouts. While COVAX aims to distribute two billion doses by the end of 2021, the program has struggled to mobilize the necessary support from wealthier nations to subsidise the initiative.

Unsurprisingly, the deployment of vaccines has raised a number of questions, including ones about what comes

next for those lucky enough to have received their shots.

Notably, states are not the only ones that are considering vaccine passports. Private companies such as airlines will likely impose movement restrictions on their customers.

There have been growing calls for digital “vaccine passports,” where those who have been vaccinated would be permitted to move around more freely. The prime minister of Greece, Kyriakos Mitsotakis, has already declared that he wants an EU-wide certificate for travel, and U.S. President Joe Biden has also asked for an evaluation of vaccination passports. Iceland has become the first country to issue and recognize COVID-19 passports, with Denmark also preparing to launch their own in a matter of months. Notably, states are not the only ones that are considering vaccine passports. Private companies such as airlines will likely impose movement restrictions on their customers. Australian airline Qantas, has already insisted that future passengers would require proof of COVID-19 vaccination before they are permitted to fly. History has shown that vaccine passports are not a radical concept. “Yellow cards” are international certificates issued by the World Health Organization, used to document vaccination against yellow fever. But what happens when vaccination efforts are largely unequal? And what are the risks or ethical implications of digitizing these passports?

WHAT COULD A DIGITAL VACCINE PASSPORT LOOK LIKE?

Digital vaccine passports currently being developed by airlines, nonprofits and tech companies are easily accessible using a smartphone. Final iterations may be an app or part of a digital wallet, potentially scanning a traveler’s facial features which then creates a biometric signature that is linked “in the cloud” to their vaccination status. IBM’s “Digital Health Pass,” would build on blockchain technology to utilize temperature checks, virus exposure notifications, test results, and vaccine status. The World Economic Forum and the Commons Project Foundation are testing CommonPass, a digital passport that would allow travelers to access testing or vaccination information; this passport would generate a QR code to share this data with authorities.

WHAT ARE THE RISKS?

Ronald Deibert, professor at the Munk School of Global Affairs & Public Policy and director of the Citizen Lab, gives us reason for caution. He remarks that, “If there’s one lesson of the digital world, it’s that it is very hard to ‘secure’ any data.” When asked about travelers’ personal information and health data remaining secure, he said, “encryption will be critical to the mission, but unfortunately many policymakers and government agencies seem intent on weakening encryption in the name of national security.” Without necessary privacy measures in place, there are huge risks of data misuse. A report from the security research company Top10VPN surveyed 65 digital health certificate apps currently in operation and found that 82 per cent had inadequate privacy policies. There are also numerous risks associated with data collection, particularly theft, manipulation, sharing, and unauthorized access by third parties. Protecting data and ensuring privacy will require additional oversight by independent agencies, which could be extremely difficult to ensure given the current lack of regulation and the scope of the passports.

ARE VACCINE PASSPORTS ETHICAL?

So how will those who are the most marginalized be affected? Due to the vaccine rollout delays and incomplete plans for vulnerable groups in lower-income countries, digital vaccine passports may add to the bureaucracy that fails to account for refugees, internally-displaced persons,

stateless people, and undocumented migrants. For countries that have failed to identify at-risk groups or have not yet started vaccination efforts, allowing freedom of movement for a portion of the global population appears ethically questionable. According to Professor Deibert, vaccine passports have the potential to exacerbate social inequalities. He states that, “people who lack the appropriate credentials or access to passports may be unable

Without necessary privacy measures in place, there are huge risks of data misuse.

to travel or work or shop while those with means may be able to purchase illicit passports, bypassing legitimate controls altogether.” Limited mobility for non-vaccinated people due to blocked travel and impeded access to employment opportunities is a likely consequence if vaccine passports are introduced before the rest of the world has a chance to “catch up” with the vaccination efforts of the West. Alternatively, the CEO of The World Travel and Tourism Council (WTTC), a forum for the travel and tourism industry, is advocating for internationally recognized rapid and cost-effective tests at departure and arrival points. Instead of punishing those who do not yet have the option of vaccination, expanded testing and more inclusive vaccination planning is needed.

WHAT’S NEXT?

It is highly likely that there will be some form of digital vaccine passports moving forward, with potentially even more intrusive forms of biomedical surveillance at border controls. However, if states and governments focus more on vaccinating the world and less on when people can move freely, there may be a more equitable outcome for society.

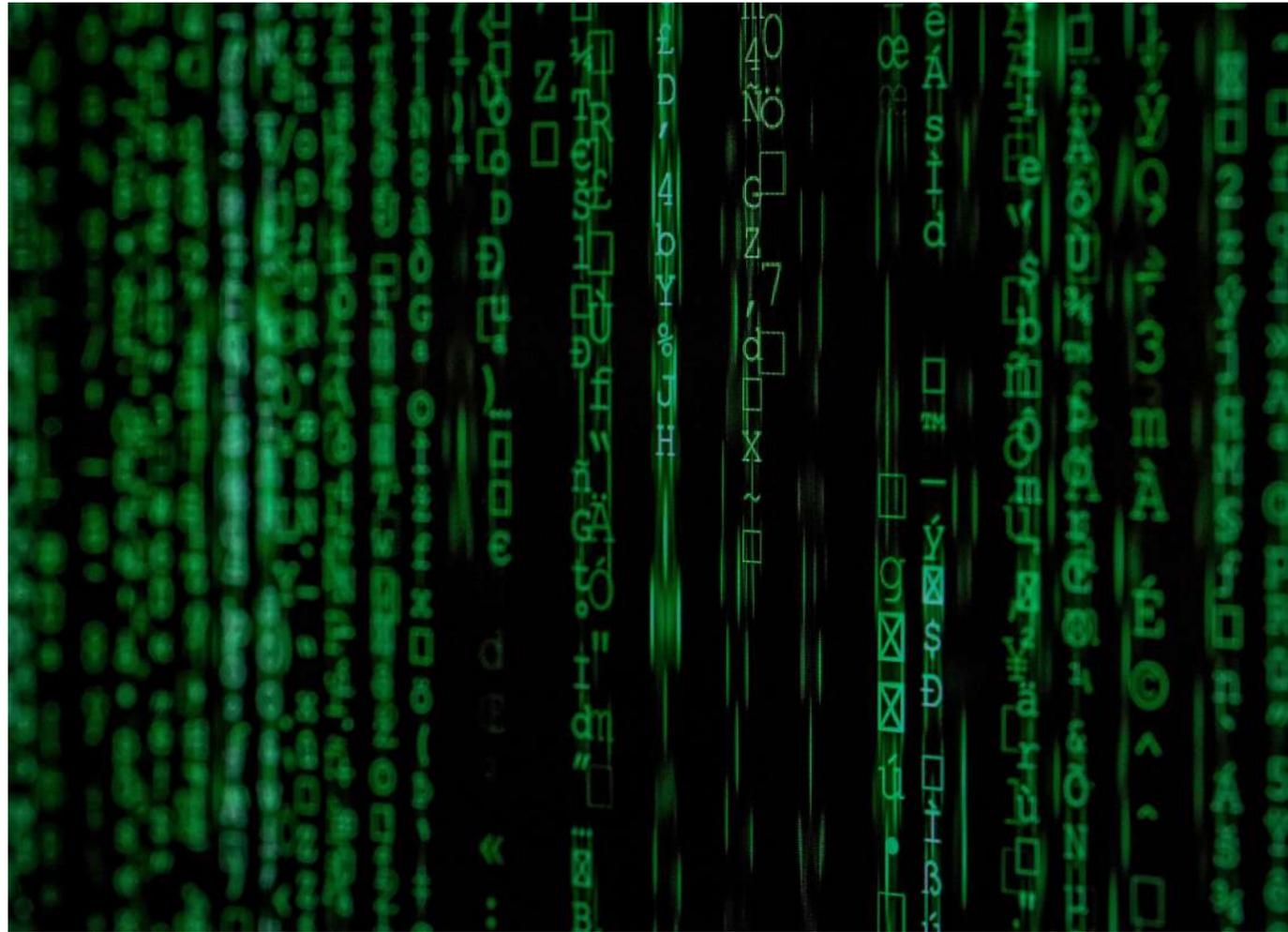


Dorottya Szekeley is a first-year student in the Master of Global Affairs program at the Munk School of Global Affairs & Public Policy. She holds an Honours Bachelor of Arts degree from the University of Toronto where she majored in Political Science, with a double minor in Sociology, and Women

and Gender Studies. Her main interests lie within the fields of global migration and refugee advocacy, as well as inter-sectional human rights. Dorottya has spent extensive time volunteering with asylum-seekers in Paris and Toronto and continues to research refugee services within Munk’s Global Migration Student Research Initiative. This past summer she served as a research and policy intern at the Canadian Centre for the Responsibility to Protect, where she focused on critical engagement with Canadian foreign policy and R2P.

Digital Authoritarianism: How Regimes Track and Silence Dissidents Across the Globe

BY JOSEPH ROSSI | HUMAN RIGHTS



TECHNOLOGY has played a formative role in advancing the human rights movement, but it has also provided a means to suppress opposition and dissent. The concepts of human rights and sovereignty have always been competing parts of the international legal landscape, which has been further challenged by a digital ecosystem that has enabled cross-border connectivity. In particular, the rise of digital access across borders has provided states with the opportunity to undermine their citizens' rights, irrespective of their physical location. This is especially the case for political activists who rely on digital platforms that subsequently make them susceptible to attacks from authoritarian governments not just in their home country, but also abroad.

AUTHORITARIAN TACTICS

With their online presence, activists can reveal information about their travel, family members, and friends—all of which can be used by malign government agents to pressure such actors. Specifically, the activists' communications with close contacts inside their home country can be intercepted and used as blackmail. In response, civil society activists have attempted to protect their digital identities, but this has engendered an aggressive response from state actors who have turned to "phishing" campaigns to obtain information about dissidents. By tricking targets into clicking on links through seemingly

official or benign digital communications, phishing allows the state to access an activist's device or obtain their confidential passwords. To pursue certain targets, government officials may even attempt to penetrate the accounts of family members or inexperienced users in activist networks. For example, an Iranian women's rights activist detailed how she was contacted via the Facebook account of her niece in a government attempt to gain access to her social media accounts.

To pursue certain targets, government officials may even attempt to penetrate the accounts of family members or inexperienced users in activist networks.

Beyond surveillance, oppressive regimes utilize online harassment, disinformation, and smear campaigns to silence dissidents abroad. In an effort to undermine their credibility, journalists and human rights activists have been portrayed as liars and accused of working with foreign governments. Additionally, activists are threatened with physical violence, assassination, or imprisonment upon return to their home country. This is especially the case for women who are targeted with misogynistic and sexually threatening insults. In certain cases, threats have been made against family members who remain in their home country; an Iranian journalist experienced this first-hand when she received a comment on one of her articles euphemistically explaining that her uncle may be the victim of an "accident."

Authoritarian governments have also used more sophisticated means to attack dissidents, like their use of spyware technology to gain access to personal information. For example, the Israeli based cybersecurity firm NSO Group and its "Pegasus" spyware have been the subject of great controversy over the past two years. This spy-

ware can infect iPhone and Android mobile device users by sending an "exploit link," a code that infiltrates a software vulnerability or security flaw to grant access to a victim's personal information such as emails and photos. Additionally, the actor using the spyware can access the phone's microphone and camera to directly spy on their target. In 2018, the Munk School's Citizen Lab released a report entitled "Hide and Seek" which examined how Pegasus spyware has been used globally. The research monitored global Internet Service Providers (ISPs) and confirmed that the tool had been used widely, with 120 ISPs in 45 countries showing signs of a Pegasus infection. In particular, the report identified numerous instances of Pegasus spyware being used to target activists, including one operator known as 'KINGDOM' who used the software to monitor cross-border activities. The KINGDOM operator was identified to be supporting the mandate and interests of the Saudi Arabian government and used the NSO Group software to target Yahya Assiri, a high-profile Saudi dissident now based in London, and an Amnesty International researcher.

This spyware can infect iPhone and Android mobile device users by sending an "exploit link," a code that infiltrates a software vulnerability or security flaw to grant access to a victim's personal information such as emails and photos.

THE CANADIAN CONNECTION

These incidents have also reached Canadian soil. One KINGDOM attack was against a dissident located in Quebec. The infected device belonged to a McGill student and Saudi political activist, Omar Abdulaziz. Since arriving in Canada to pursue his education, he has been an outspoken critic of the Saudi government which had drawn the ire of the hardline Middle Eastern Kingdom. While a student at McGill, Abdulaziz created a YouTube channel where he criticized the Saudi government's repressive tactics and violation of human rights. In 2018, the Saudi government responded by threatening Abdulaziz's brother with jail time, and after he continued to voice his discontent with the home government, two of his brothers and a number of his friends living in Saudi Arabia disappeared. This was made possible by Pegasus accessing Abdulaziz's contacts, family photographs, instant messages, and voice calls.

PHOTO SOURCE: UNSPLASH, MARKUS SPISKE

FORMING PARTNERSHIPS

The case of Omar Abdulaziz is just one of numerous examples of the malicious and targeted use of Pegasus spyware. With autocratic states finding new and creative ways to exploit technological advancements to suppress the rights of its citizenry, countries that are interested in protecting and advancing human rights and freedom of expression have begun to formulate an effective strategy to combat these practices. One effective mechanism is public-private partnerships, such as that found in American cybersecurity. In the United States, the public and private sectors partnered to take down botnets, computer networks infected with harmful software that enables individuals to access and control computers remotely. In 2013 for example, Microsoft and the Federal Bureau of Investigation (FBI) worked together to disrupt botnets which infected computers with “Citadel” malware that led to financial fraud. This collaborative relationship may enable both the public and private realms to utilize their sector-specific knowledge and experience to protect the personal devices of individuals threatened and repressed by their home government.

This spyware can infect iPhone and Android mobile device users by sending an “exploit link,” a code that infiltrates a software vulnerability or security flaw to grant access to a victim’s personal information such as emails and photos.



Joseph Rossi is a first-year student in the Master of Global Affairs program at the University of Toronto. He completed his undergraduate degree at the University of Toronto in International Relations. As an undergrad, he was a Crisis Analyst for the North American Model United Nations, Vice-President of the Italian Undergraduate Student Cultural Association and a journalist for *The Varsity* newspaper. His research interests include Canadian foreign policy, inter and intra-state conflict and international organizations.

Spyware has enabled authoritarian regimes to monitor and threaten citizens irrespective of their physical location. Actions such as these undermine the basic human right to freedom of expression and endanger dissidents raising valid criticisms of their home countries. Without activists sounding the alarm about abuses around the world, the international community would remain in the dark about government-sanctioned human rights abuses, and could do little to address such violations. Enacting regulations to prevent the misuse of private software for government repression is increasingly important to protect the voices of human rights defenders and journalists, wherever they may be.

Social Media’s Role in Political and Social Movements in Africa

BY REBECCA SEWARD-LANGDON | SUB-SAHARAN AFRICA

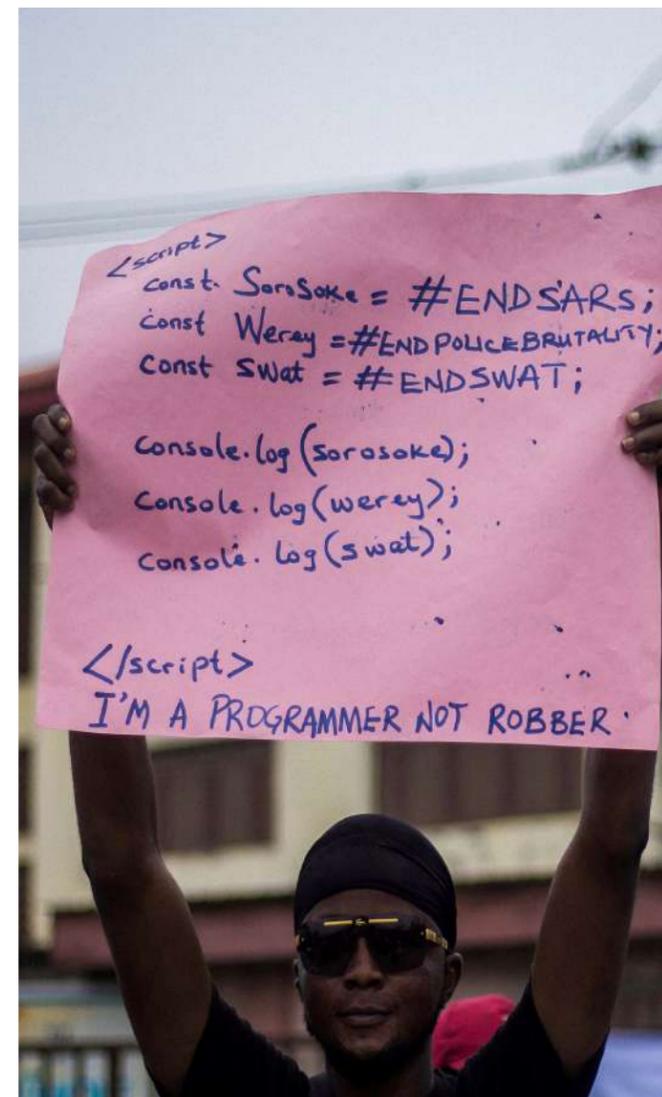


PHOTO SOURCE: UNSPLASH, OMOTAYO_TY

SOCIAL media has changed the political sphere in Africa, from the 2011 Arab Spring to 2020’s #EndSARS and #RedPearlMovement campaigns. Growing youth populations, new technologies, and increasingly accessible online platforms make social media a popular tool in grassroots movements. But just how successful is social media in achieving social change? A closer look at some of the most recent online movements in Africa details the achievements and shortcomings of online activism on the continent.

THE ROLE OF SOCIAL MEDIA

At its core, social media provides a new space for public discourse. Where media censorship and state violence prevail, citizens have used online tools to hold governments accountable and attract international attention.

When mainstream media can no longer be trusted due to state ownership or censorship, social media outlets become platforms for sharing critical information.

Videos and live streams in particular are catalysts for online movements because they can show human rights violations or humanitarian crises in graphic detail.

When mainstream media can no longer be trusted due to state ownership or censorship, social media outlets become platforms for sharing critical information. For example, information spread through WhatsApp and Facebook was crucial to the Egyptian protests of 2011. Protestors now use online platforms to spread information beyond national boundaries as well, attracting worldwide attention to their causes.

NIGERIA’S #ENDSARS MOVEMENT

Nigeria’s Special Anti-Robbery Squad (SARS) is known for profiling young people as criminals, often with vio-

lent consequences. In October 2020, a video of a SARS police officer shooting a young man went viral. With their large presence on Twitter and pent-up anger from being the targets of illegal arrests, Nigerian youth took to social media and the streets to demand an end to police brutality.

There was a brief period without major clashes with protestors following the Lekki Massacre, indicating the international attention might have helped reduce police violence for a short time.

Just over a week later, the Inspector-General of Police announced that it would dissolve SARS. However, the Public Relations Officer of the Nigerian Police Force later said that a Special Weapon and Tactics (SWAT) team would replace SARS, with no indication that any of the protestors' demands would be met. In an attack on October 20, armed soldiers opened fire on protestors at the Lekki Tollgate in Lagos. Disk jockey DJ Switch live-streamed the shootings on Instagram, while other protestors uploaded videos to Twitter and Facebook.

The Lekki Massacre was the tipping point that garnered worldwide attention. Protestors reported via social media, while celebrities and mainstream media outlets shared news about the #EndSARS movement as well. Women took the lead with Feminist Coalition, a women's group committed to amplifying the voices of Nigerian youth. The coalition used social media and online crowdfunding to raise money for medical, legal, and memorial costs for protestors.

Quickly, international organizations including the United Nations and Amnesty International were demanding

justice for Nigerians. Sympathetic protestors demonstrated at the Nigerian High Commission in Ottawa, as well as in the United Kingdom and other nations. This put pressure on the Nigerian government. There was a brief period without major clashes with protestors following the Lekki Massacre, indicating that international attention might have helped reduce police violence for a short time. However, police once again beat and arrested protestors at the Lekki Tollgate in February 2021, drawing renewed attention to the issue.

The original five demands were never met, and SARS was simply replaced by SWAT. The root causes of police brutality in Nigeria do not start and end with SARS. As protestors have pointed out, police violence is intertwined with the improper use of power, poor governance, low salaries, and the systematic marginalization of young people. Ultimately, the #EndSARS movement suggests that social media alone is not enough to make large-scale changes; it can only spread information far enough for international actors to offer their support in more effective ways.

UGANDA'S #REDPEARLMOVEMENT

In the lead-up to Uganda's 2021 presidential election, Ugandan youth used the hashtags #RedPearlMovement and #WeAreRemovingADictator to support opposition candidate Bobi Wine. His supporters shared information about the elections and encouraged Ugandans to vote President Yoweri Museveni out of office. Museveni, who has been president of Uganda since 1986, was campaigning for a sixth term despite passing the presidential age limit of 75.

In November 2020, police arrested Bobi Wine for allegedly violating COVID-19 protocols during his campaign. Protestors who took to the streets of Kampala were met with violence from security forces. At least 45 people died from gunshot wounds and many more were injured.

This was followed by a nation-wide lockdown and internet blackout designed to stop protestors from gathering. Ugandan youth turned to social media to fight back and called on international supporters to share what was happening. The posts shared by the Red Pearl Movement stressed that online presence and solidarity would prevent further state violence.

Thanks to the online support, Spotify published a podcast series called The Messenger that highlighted Bobi Wine's fight for freedom. The Media Freedom Coalition also released a statement condemning the social media blockages that were endorsed by the governments of Canada, the United Kingdom, the United States, and many others.

Ugandan youth turned to social media to fight back and called on international supporters to share what was happening.

The High Court of Uganda may have considered Bobi Wine's online support before ruling that his detention was unlawful. However, police continue to monitor his whereabouts. There is no doubt that the online support attracted international attention, including from the U.S. State Department, which is "considering a range of targeted options." These measures include visa restrictions for those responsible for undermining the democratic process.

In Uganda's case, social media successfully spread information to actors powerful enough to hold those responsible accountable for their actions. Although pressure from the international community may have limited unconstitutional arrests, their public statements did not lead to a peaceful transition of power. This may be another limitation of activism on social media, as it can get information to outsiders but cannot induce them to take direct action.

IS SOCIAL MEDIA AN EFFECTIVE TOOL?

Online activism can only get a movement so far. The #EndSARS and #RedPearlMovement examples show where social media ends, and real change begins. Social media plays a role in coordination and in spreading a message worldwide, but it is left to international actors to apply the required pressure. However, international actors may be wary of intervening and undermining a

state's sovereignty or reluctant to take direct action. This presents significant limitations on affecting change.

Still, online activism is not useless. Online platforms make it easy to connect with people worldwide as information can spread through networks of international supporters. When gathered by active protestors and reporters, this information is very frequently up-to-date and reliable, especially when speaking from perspectives that are silenced by the government. Social media will be an important tool for Africa going forward—but it cannot be the only one.



Rebecca is a first-year student and the Munk School of Global Affairs & Public Policy. She completed her undergraduate degree in African Studies and Political Science at Carleton University. Her interests include China-Africa relations, environmental

conservation, and African independence. At the fourth Annual African Studies Undergraduate Conference, Rebecca presented her research on community efforts of environmental conservation in Tanzania and Rwanda after visiting the two countries, and co-hosted the event the following year. During her undergraduate studies she wrote an honours research essay on the effects of China's non-interference policy in Africa and assisted in the Rethinking African Liberation research project. Search engines are commonly viewed as the go-to resource to find information and answers to our daily questions. What users often do not realize, however, is that Google—the number one search engine in the world—holds significant power over the type of search results they see and can alter results based on specific user data.

Search Engines and the Power They Hold: Google's Role in Perpetuating Hate Speech, Racism, and Sexism Online

BY KATHERINE ROSS | TECHNOLOGY AND INNOVATION



ALGORITHMS of Oppression: How Search Engines Reinforce Racism, a book by UCLA Information Studies Professor Safiya Noble, exposes how big tech companies and their search engines—particularly Google—perpetuate racism, sexism, and other biases. For instance, when searching “Black girls,” “Asian girls,” or “Latina girls,” in Google’s search engine, Noble noted that the resulting images were almost exclusively pornographic or hypersexualized. Conversely, when Noble searched “white girls” and “white teenagers,” the search results displayed friendly, wholesome, and all-American images. This is only one example of how search engines and data can be manipulated to misrepresent women of colour and perpetuate racism, sexism, and associated biases.

Since this revelation, large corporations have been under

pressure to improve their technologies’ deep-seated biases. Big tech companies, such as Google, have made public efforts to correct the racist, sexist, and biased functionalities of search engines after experiencing heightened scrutiny following the publication of Noble’s findings. Yet, unfortunately, Google continues to propagate disinformation, hate speech, and anti-democratic conspiracy theories by providing users with a platform to spread their views.

HOW GOOGLE CATERS TO THE USER

Google’s search engine technology has mass-personalization capabilities that cater results based on personal data, previous searches, links clicked, current location, and more. As a result of rising public concerns over data

privacy, Google has become marginally more transparent about how the corporation capitalizes on personal data to cater paid ads to specific types of users based on their preferences. Google’s ad personalization website allows users to view what tags are associated with their online presence. Personalized tags include information like a user’s age, gender, whether or not they play violent video games, which organizations they have searched for, their favourite sport teams, videos they watched, their cell phone service provider, and more. Through these ad personalization capabilities, users can be tagged and connected with certain groups and continuously exposed to information that aligns with the views shared by a particular demographic. For instance, studies show that YouTube—which is owned by Google—allowed white supremacists and other hate groups to recruit and speak freely about their violent ideologies on its platform.

Through these ad personalization capabilities, users can be tagged and connected with certain groups and continuously exposed to information that aligns with the views shared by a particular demographic.

Given that Google not only has access to user’s personal data but also the ability to cater search results based on that data, the results to a single search may differ between users due to their different tags and preferences. This is problematic as it reveals that Google’s search engine is not value-free and the design behind Google’s search algorithms influences users’ experiences. This means that Google’s search algorithms are not “just math,” as is commonly suggested.

With the world currently facing a severe global health crisis, access to reliable information is even more important than before. With many traditional resources such as libraries, schools, teachers, universities, and in-person learning increasingly inaccessible due to COVID-19 restrictions, the internet has overwhelmingly become the leading source of information, worldwide. The inaccessibility of many other trusted and essential sources of information may be exacerbating the issue of disinformation on the internet.

WHAT’S THE OTHER SIDE OF THE COIN?

A common response to these issues is the claim that Google cannot limit the amount of hate speech, racism, sexism, and bias that exists online because it would infringe upon individuals’ freedom of speech and freedom of expression. That’s up for debate. In Canada, the Charter of Rights and Freedoms permits the government to enforce “reasonable” limits on certain rights. While Canadians have a right to freedom of expression, hate speech, obscenity, and defamation are restricted in Canada.

However, in 2016, Google went to the Supreme Court of Canada to defend the right to freedom of expression online. Google was accompanied by numerous high-profile rights organizations including Human Rights Watch, the Canadian Civil Liberties Association, and the Electronic Frontier Foundation to support the corporation’s stance on allowing all speech online. The rights organizations argued that by restricting content available online, the Canadian government was restricting freedom of expression. Google sought to overturn a ruling which it claimed set a precedent for countries to use their courts to block worldwide access to any domestically disapproved internet content. On April 16, 2018, a judge of the British Columbia Supreme Court dismissed Google’s motion. Google and human rights organizations contended that the ruling was a great risk as it justified censorship and restricted freedom of expression online.

In the U.S., free speech on the internet involves a more fruitful debate. Many ask where the line should be drawn between free speech and hate speech. If Google begins to remove certain websites, videos, and posts because they are allegedly spreading racist, sexist, or

PHOTO SOURCE: UNSPLASH, SOLEN FEYSSA

With the world currently facing a severe global health crisis, access to reliable information is even more important than before.

hateful narratives, the corporation can expect pushback from those claiming that removing specific content from the internet is an infringement of the freedom of speech.

WHAT CAN BE DONE?

In our digital world, search engines and the algorithms that drive them increasingly decide what we see. It is important to remain critical of information found online, especially considering that Google has the ability to cater specific websites and information to users based on their data. Users must understand the whole host of attendant power issues associated with these technologies and how to protect the public from the extractive models foisted upon society by big tech companies, especially Google.

The internet can make it difficult for users to discern sources of truth, especially when information is catered based on data, beliefs, or gender, and the results that many users consume are vastly different from those consumed by others. This issue is exacerbated when white supremacists and other hate groups are granted unfettered use of the internet as a domain to spread hateful narratives. Consequently, there are extreme dangers of groupthink at play when Google's search engine influences users' search results, ultimately altering one's perceptions of reality.

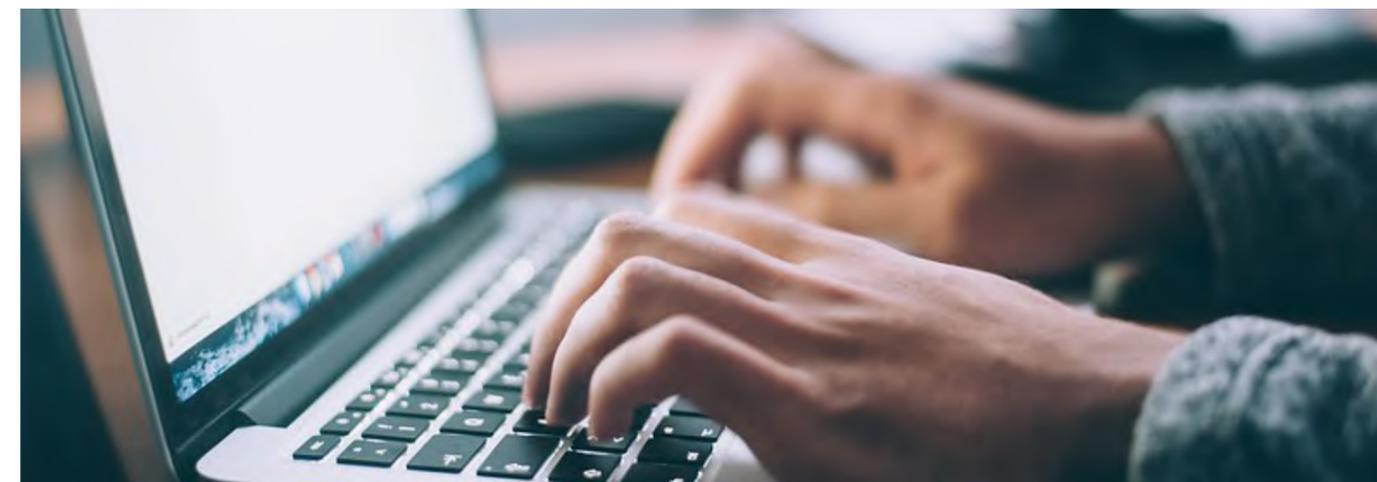


Katie is a second-year Master of Global Affairs candidate at the Munk School of Global Affairs & Public Policy. She also graduated from Western University with an Honours Specialization in Media, Information & Technoculture.

This summer, Katie worked at MaRS Discovery District, the largest innovation hub in North America, where she advised on their marketing strategies by analyzing their data analytics and provided tailored recommendations on how to improve their outreach to increase the number of ventures and small businesses in the MaRS ecosystem. She has research interests in artificial intelligence ethics, data governance and security, international space policy, space governance, and national and international foreign and defense policy.

How Pandemic Lockdowns Enabled the Weaponization of the Internet Against Women

BY JULIA DA SILVA | GENDER AND IDENTITY POLITICS



SINCE the beginning of the pandemic, the internet has seen a surge in traffic. The majority of our daily activities have been reimaged virtually, whether through the use of remote working tools like Slack, or through video conferencing platforms such as Zoom. Websites like Facebook, YouTube, and Netflix have also seen major spikes in their number of users during the pandemic. Our new digital reality has led us to experience what a study in Human Communication Research calls, “online vigilance,” which consists of three main components: constantly thinking about the online world, continuous observation of online content via multiple devices, and instantly reacting to notifications.

As a result of the pandemic and emergency stay-at-home orders worldwide, online vigilance has become a way of life for millions, especially when an online presence is required for those working remotely. Constant digital connection has led to an increased amount of stress in people's daily lives. According to the Centre for Addiction and Mental Health, women are dealing with higher rates of anxiety and loneliness than men during the pandemic, much of which is due to constant online activity.

DIGITIZING TRAUMA

In many cases, women are navigating their new digital reality while experiencing or reliving significant trauma.

A recent survey from Plan International found that more than half of young women and girls have experienced online abuse such as cyberstalking, threatening messages, and unwanted explicit images. Plan International spoke to 14,000 young women and girls aged 15-25 in 22 countries, finding that approximately 20 per cent of them had left social media and another 12 per cent adapted their internet usage to avoid further online harassment and abuse. Unfortunately, the global pandemic has forced many women who had previously left social media for their own personal well-being to return to this digital world.

Yet, it is difficult for women to adapt their online usage when digital crimes have been steadily increasing throughout the pandemic. The internet has become weaponized by predators to harm women, resulting in a rise in stalking and harassment, both online and in-person. More people (especially minors) have been reaching out to law firms for assistance in cases of sexual extortion and abuse. Notably, many of these instances are not new cases of digital harassment. For many women, this new online reality is forcing them to relive past trauma, resulting in unprecedented levels of stress and anxiety.

Survivors of online sexual abuse including stalking, harassment, revenge porn, and sexual extortion are now being told that the digital world is a saviour during the COVID-19 pandemic, when for them it is a source of pronounced anxiety and trauma. Many survivors are ex-

PHOTO SOURCE: FLICKR, RYAN MORSE

periencing symptoms of PTSD, anxiety, insomnia, flashbacks, numbness, and nightmares as they navigate this now-essential digital world.

In this new digital world more women are feeling forced to be on camera in order to appear credible and assert themselves in professional or academic settings.

TOWARD A WELCOMING DIGITAL SPACE

With growing numbers of women (re)living the trauma of online abuse, it is easy to see how difficult it is for young women to navigate an online space where abuse is so prevalent. But for many, especially those attending school and working online, the digital landscape is unavoidable. This new reality has led scholars and theorists to think about ways to resist the norms of our online existence.

Francesca Rossi, a psychotherapist in New York City that works with survivors of digital violence, has coined the phrase: “affirmative camera consent,” which challenges the way that we proceed with our online culture. Before any online event, whether a class, meeting, or a social call, Rossi asserts that participants should be asked if they are truly comfortable with being on camera, ideally while the event is still being planned. In this new digital world more women are feeling forced to be on camera in order to appear credible and assert themselves in professional or academic settings. Being on camera can be difficult and triggering for many survivors of abuse and it should never be the reason why they cannot attend an online event.

Another useful tactic for dealing with online spaces that are potentially harmful to women is the notion of bystander intervention. For digital situations where negative attitudes toward women and/or sexual violence are expressed, bystander intervention could be a way for women to safely ease into digital spaces. These bystander interventions could involve calling out sexist language, questioning the portrayals of women and girls in the media and on social networking platforms, and challenging the use of pornography.

Bystander intervention is a tangible solution that could easily be applied to various online contexts. For instance, professors and TAs could speak up at the start of the semester to communicate that online harassment will not be tolerated. This would be especially meaningful in the context of online school and would set a worthwhile precedent about acceptable behaviour in this environment. Likewise, at online social events, attendees could intervene if others are creating an unsafe environment. Immediate intervention to address sexist or unwelcome behaviour helps create an environment where everyone knows that social norms that encourage violence against women are not permitted.

The transition to online living has emboldened many to weaponize the internet in order to harm women. Measures such as affirmative camera consent and bystander intervention demonstrate that there are tools that can help protect women from harassment and allow their allies to create safe online spaces for work, learning, and fun.



◇

Julia Da Silva is a first-year Master of Global Affairs student. She completed her undergraduate degree at the University of Ottawa in International Development and Globalization with a Minor in Women's Studies. Julia has worked with Crown-Indigenous Relations and Northern Affairs Canada and Polar Knowledge Canada. As an undergrad, she was the Delegate Coordinator for the University of Ottawa's International Development Week Conference and part of the International Development Student Association's Mentorship Program. She has been a Parliamentary Assistant in the House of Commons. Most recently, Julia worked at Women and Gender Equality Canada.

Digital Disease: Understanding the Online Spread of Anti-Vaccination Sentiment

BY ALEXANDREA JOHNSTON | GLOBAL HEALTH



ANTI-VACCINATION sentiment cannot be taken lightly. In 2019, the World Health Organization (WHO) named vaccine hesitancy one of the top ten threats to global health. Doubts around the safety and effectiveness of vaccines persist despite the fact that vaccinations are proven to be one of the most successful public health initiatives. This growing anti-vaccination movement has contributed to decreasing vaccination rates in Europe and the United States, particularly among small communities that are more vulnerable to disinformation. Anti-vaccination sentiment has grown substantially during the COVID-19 pandemic, partly due to the movement's increased mobilization through digital means.

DIGITAL DISINFORMATION

While vaccine hesitancy is characteristic of small portions of societies, the anti-vaccination movement has gained significant traction. Its impact has been severe, resulting in lowered global immunity to certain diseases and increased virus outbreaks. For example, the United States experienced a ten per cent decline in the number of parents who say it is very or extremely important to vaccinate their children, from 94 per cent in 2001 to 84 per cent in 2019. Additionally, administration of the second dose of the measles-mumps-rubella (MMR) vaccine has fallen

to 87 per cent in the United Kingdom, well below the 95 per cent immunization rate required for herd immunity. It is important to note that there is a distinction between the anti-vaccination movement and vaccine hesitancy.

It is estimated that COVID-19 has resulted in an increase of roughly eight million new followers of social media accounts supporting anti-vaccination sentiment.

Meanwhile, the WHO defines vaccine hesitancy as a “delay in acceptance or refusal of vaccines despite availability of vaccination services.”

PHOTO SOURCE: FLICKR, GOTOVAN

The increase in anti-vaccination sentiment in recent years can be largely attributed to the proliferation of disinformation on social media through algorithms that highlight popular content or recommended pages. Specifically, platforms like Facebook, Twitter, and YouTube have large groups of anti-vaccination supporters which have grown substantially throughout the COVID-19 pandemic. It is estimated that COVID-19 has resulted in an increase of roughly eight million new followers of social media accounts supporting anti-vaccination sentiment. These accounts now boast approximately 58 million followers in total. The largest anti-vaccine audience can be found on Facebook, followed by YouTube, Instagram, and Twitter.

Digital platforms encourage the rapid sharing of user-generated content, a practice which does not lend itself to vetting or fact-checking. This is particularly concerning as it allows for easy access to misleading or false information. The consequences are dire, given that more and more people are turning to online sources for health information and news. A 2012 article found that 80 per cent of internet users search for health information online, while 16 per cent search specifically for vaccination information. 70 per cent of individuals claim that the information they found influenced their treatment decisions.

USING DIGITAL PLATFORMS TO COMBAT DISINFORMATION

While the rise of social media platforms has contributed to increased anti-vaccination sentiment, these digital platforms can also be used to curb it. Despite the fact that the vast majority of the global population complies with vaccinations, vaccine supporters rarely speak up. This silence is often compounded by delayed action on the part of social media companies to remove posts or label them as fake. Given this reality, a digital campaign encouraging vaccine supporters to speak up and address false information would dramatically assist in curbing the spread of anti-vaccination sentiment. Ultimately, addressing the concerns of those who are hesitant about vaccination does not boil down to facts or logic. Rather, it depends upon communication. A recent study published in *Nature* magazine assessing online views of vaccination concluded that, “although smaller in overall size, anti-vaccination clusters manage to become highly entangled with

undecided clusters in the main online network, whereas pro-vaccination clusters are more peripheral.” The study warned that the anti-vaccination movement could eventually overwhelm the pro-vaccination movement, the devastating consequences of which would last well beyond the COVID-19 pandemic.

Social media platforms and governments need to encourage people to speak up when they see false information shared online about vaccinations. By increasing the availability of factual information on false posts, those who are undecided about their decision to vaccinate themselves and their loved ones against COVID-19 or other preventable diseases will be presented with both sides of the argument when searching for information online. People need to see the consequences of not vaccinating, not just through data but through personal narratives and imagery which individual vaccine supporters can help provide.

While the world is already burdened by a pandemic, economic crises, and fractured social cohesion, the importance and the danger of anti-vaccination sentiment cannot be ignored. With people now spending more time on social media than ever before, the spread of digital disinformation can begin to be combated by leveraging the voices of the millions of vaccination supporters on these platforms. This will be critical moving forward not only from the COVID-19 pandemic, but in preventing future pandemics as well.



Alexandrea Johnston is a first-year Master of Global Affairs Student. She obtained her Bachelor of Science from McMaster University majoring in Psychology, Neuroscience, and Behaviour, and minored in Sustainability. As an undergrad, Alex was heavily involved in McMaster student life serving in multiple roles for her program and faculty societies. Additionally, Alex spent time researching in the field of neurolaw and conducting research for the City of Hamilton. Alex has spent summers interning both in Canada and globally in the financial sector, commercial insurance, and legal fields. Before coming to Munk, Alex spent a year serving the 25 000 Undergraduate students at McMaster as the first female Vice-President Finance for the McMaster Students Union.

How Social Media Became the Digital Battleground in the Fight for American Democracy

BY KRISTEN PEARN | NORTH AMERICAN AFFAIRS



PHOTO SOURCE: FLICKR, CHAD DAVIS

IN the months leading up to the 2020 American presidential election, national polls projected that Democratic Party candidate Joe Biden would win both the popular and electoral majority vote over the incumbent, Donald Trump. In the face of political uncertainty, President Trump renewed his efforts to disenfranchise Democratic voters and pre-emptively delegitimize the election results. Amid the COVID-19 pandemic, President Trump and many Republicans repeatedly claimed that mail-in and absentee ballots would lead to mass corruption and voter fraud. They imposed a raft of measures designed to deter voting, including voter ID requirements, limits on early voting, closing polling locations in lower-income areas, and purging voter rolls. Despite the Republican Party’s voter suppression tactics, President Trump lost the Electoral College and his subsequent lawsuits challenging the election outcome in several swing states. As the defeats piled up, President Trump persisted with his “voter

fraud” strategy, tweeting a barrage of baseless claims and conspiracy theories which perpetuated an atmosphere of political polarization and conflict.

President Trump’s election fraud narrative has been a part of his playbook for years. When Barack Obama was re-elected in 2012, Trump claimed that the entire election was a “total sham.” In 2016, Trump alleged that Senator Ted Cruz stole the Iowa primary and that Hillary Clinton did not win the popular vote in the general election because “millions of people voted illegally.” Trump’s penchant for disinformation—first emerging with the ‘birther’ conspiracy theory surrounding Obama’s birthright citizenship—culminated around the 2020 election as he leveraged his robust social media apparatus to mobilize his base.

SOCIAL MEDIA ALGORITHMS AND DISINFORMATION

Trump's tactics were made possible by the market shift from traditional media sources, such as print publications and broadcast news, to social media platforms. Facebook, Instagram, Twitter, YouTube, and similar apps have afforded millions of people the opportunity to connect and communicate instantaneously. The premium placed on consumer interaction has incentivized social media companies to adopt questionable ethical practices, such as the collection and sale of user data, to maximize consumer engagement and operational growth. Many social media companies harvest data on unwitting users to refine their advertising techniques and fuel their recommendation engines, encouraging users to connect with like-minded individuals and groups. The division of mass audiences into small factions based on shared interests has promoted human connection, but has also stoked extremist beliefs and contributed to societal polarization.

President Trump's incessant claims of election fraud sowed the seeds for widespread conspiracy theories to take root in the social media ecosystem. Misleading voting maps of swing states were posted as evidence of fraud on 8kun, a message board known for its extreme content. These allegations fueled the conspiracy theory that Democrats and the "deep state" had engaged in a coordinated effort to steal the election, a claim that was circulated by factions of Trump supporters, right-wing extremists, and Russian bots and troll farms. These factions were then grouped together by social media algorithms, which allowed proponents of various conspiracy theories—ranging from 9/11 "Truthers" to QAnon—to unite in their battle against an alleged global cabal of corrupt world leaders and elites. Some of these conspiracies made their way into the president's public utterances, the chambers of Congress, and the programming of right-wing news networks like Fox News, One America News (OAN), and Newsmax. The constant bombardment of conspiracy theories and disinformation has fueled cynicism about the mainstream media and has made it increasingly difficult for the average user to discern fact from falsehood.

According to Dr. Alison Meek, a professor and expert on U.S. conspiracies at the University of Western Ontario, the spread of conspiracy theories on social media has

long been difficult—if not impossible—to regulate. She asserts that by facilitating instantaneous communication, fostering a sense of community, and providing a space to share grievances and plans, social media has exacerbated the explosion of conspiracy theories across the world.

President Trump's incessant claims of election fraud sowed the seeds for widespread conspiracy theories to take root in the social media ecosystem.

The real danger, Dr. Meek argues, lies with those who adhere to conspiracy theories online, then decide to seek their version of justice in the real world. Dr. Meek claims that the January 6 attack on the U.S. Capitol exemplifies this threat and prompted the FBI's recent decision to classify some extremist movements, including QAnon, as domestic terrorist threats.

THE ISSUE OF CENSORSHIP

The attack on the U.S. Capitol provoked a visceral reaction from Democrats in Washington, who had repeatedly warned social media companies of the dangers posed by the largely unchecked spread of malicious content on their platforms. In response to mounting political pressure, Twitter permanently banned Trump's account and purged more than 70,000 conspiratorial QAnon-affiliated accounts, citing violations of the company's civic integrity policy. Facebook and Instagram followed suit, banning Trump's accounts through the presidential transition and removing hundreds of pages and accounts associated with the spread of disinformation. YouTube suspended Trump's channel and declared it would issue strikes against any channel posting videos about voting fraud and violating the platform's policies. Donald

Trump's removal from numerous social media platforms received mixed reactions among Washington officials, media analysts, and world leaders.

Many Washington officials viewed the social media companies' aggressive action as long overdue, while critics pointed to the dangers of censorship. Some analysts have suggested that censoring Trump supporters and right-wing extremists will only force them to migrate to more homogenous and unregulated platforms, such as Parler and TheDonald. World leaders including German Chancellor Angela Merkel, Mexican President Manuel Lopez Obrador, and British Prime Minister Boris Johnson, described the companies' actions as "problematic." They asserted that only lawmakers, not social media CEOs, have the authority to regulate freedom of speech.

GLOBAL IMPACT

While the U.S. has been reluctant to rein in 'big tech' due to fears of state overreach and a constitutional commitment to free speech, it must identify clearer regulatory responsibilities to mitigate the threat that online platforms pose to societies. Whatever course of action it chooses, the U.S. government's decision will have global socio-political repercussions. The impact of disinformation has already been felt around the world. During the 2016 Brexit referendum, Boris Johnson promoted unfounded claims that the country would reap billions of pounds upon leaving the European Union. That same year, a pro-Kremlin internet research agency exploited social media factionalism to spread disinformation and interfere in the U.S. presidential election. More recently, cyber armies spread disinformation to influence the 2019 Indian election campaign. These incidents have contributed to a growing international consensus that the structural design of social media platforms not only presents ample opportunity for exploitation, but poses an inherent threat to democracy worldwide. Stricter federal regulation of social media platforms is a necessary first step to mitigate the spread and impact of disinformation.

The U.S. government must take caution in surveilling, investigating, or criminalizing American citizens based on their ideologies, no matter how repugnant. Still, there is potential for a middle-ground approach that protects Americans' freedom of speech while avoiding the pitfalls of censorship. Such an approach could entail imposing

regulations which mandate social media companies to protect user privacy, improve transparency in online advertising, and curate content more ethically, so that factual information rises to the top. The U.S. government can also enact policies forcing social media platforms to moderate their content through fact-checking and contextualizing information. An American digital sphere grounded in factuality and transparency is attainable. With the right top-down policies, the four-year disinformation campaign precipitated by Trump and his allies can be rolled back.



Kristen Pearn is a first-year student in the Master of Global Affairs program at the University of Toronto. She completed her undergraduate degree at the University of Western Ontario in History and Criminology. As an undergrad, she maintained a starting position on the Western Mustangs Varsity Softball team and a part-time position both as a Research Assistant and volunteer at a local charitable organization. She then completed her Master's degree at the University of Toronto in History. As a Master's student, she specialized in U.S. Cold War foreign policy and civil rights and worked part-time as a Teacher Assistant.

Europe Confronts Tech Giants Over Consumer Protection and Content Moderation

BY PIERRE MILLER | EUROPEAN AFFAIRS



THE Digital Services Act (DSA) and the Digital Markets Act (DMA) are the latest buzzwords to come out of Brussels. Behind these obscure terms lies the next ambitious set of regulations for digital technologies in the European Union (EU), building on the landmark General Data Protection Regulation (GDPR) of 2016.

Tech giants know that the stakes are high. Google, Facebook, Apple, and Amazon have been lobbying intensely in hopes of watering down the two new directives. Simultaneously, some national governments have been encouraging the European Commission to step up its efforts to rein in the digital platforms. The result is likely to be a new power struggle with massive shows of strength between governments and tech giants.

Politicians and the European public are growing increasingly concerned about the power and influence these companies can assert over their lives.

PHOTO SOURCE: FLICKR, EUROPEAN PARLIAMENT

The first characteristic of the new set of rules outlined by the European Commission is their deliberate asymmetry. They target large companies more stringently than smaller ones—a distinction used to single out American tech giants. Politicians and the European public are growing increasingly concerned about the power and influence these companies can assert over their lives. They also see them as monopolistic foreign competitors, since there is not a single European company that can break their stranglehold over the social network, communications, and online shopping services markets. European citizens are increasingly dependent on American companies, raising concerns about sovereignty and consumer protection. These digital monopolies could prove dangerous, as they allow firms to collect data on the preferences and behaviour of their consumers with a degree of accuracy that rivals the capabilities of government agencies.

WHY TECH COMPANIES ARE WORRIED

While concerns over consumer protection and sovereignty are valid, there are reasons for tech companies to feel anxious about the EU's proposed draft regulations. The proposal suggests that large online platforms should be subject to new limitations that prevent the development of monopolies and strengthen competition. If passed, they would ban practices that companies currently use to get an edge over their competitors, such as displaying proprietary products first in search results or restricting access to their online marketplaces. Mergers would also be made more difficult. Further, the penalties for failing to comply could be steep. The European Commission could impose fines of up to ten per cent of a company's global revenue, or even break up companies altogether in extreme circumstances. Similarly, Brussels plans to implement hefty sanctions for companies that are unable to contain the spread of "illegal content," a broad term that includes not only counterfeit materials, but also hate speech. As a result, tech giants have chosen to fight back. Anxiety over the proposed regulations has led them to spend tens of millions of euros to finance lobbying efforts and fund studies that demonstrate the high costs associated with the DSA/DMA. Google alone has organized more than 160 meetings with officials from the EU.

National regulators would also be provided enhanced powers regarding content moderation, allowing them to directly impose fines on firms that do not respect Euro-

pean guidelines. However, national regulators have been reluctant to impose penalties either due to their limited capacities or a general lack of will. This has been the case in Ireland, where many tech giants have established their headquarters and brought with them secure, high-paying jobs. Due to its dependence on the presence of technology companies such as Facebook, Google, or Twitter for employment, the island nation may be concerned about retaliation if regulations became more strictly enforced. To avoid such a scenario, the EU is planning to establish a European Board for Digital Services that would oversee regulators and take action on their behalf.

However, content removal is so controversial that Facebook had to create a 'supreme court' where 20 members deliberate over difficult cases of moderation.

Companies will likely have difficulty implementing new regulations on the sale of illegal or counterfeit products proposed in the DSA/DMA. For instance, eBay mainly acts as a marketplace and has very little power over the sellers and merchandise on its platform. Reducing the proliferation of illegal content is also a challenge for many platforms, as public authorities often change their position regarding the role of marketplaces, social networks, and the question of content moderation more generally. Germany passed the Network Enforcement Act in 2017, allowing its moderators to delete thousands of posts each month. The U.K. has also submitted its own proposal to regulate illegal content. However, content removal is so controversial that Facebook had to create a 'supreme court' where 20 members deliberate over difficult cases of moderation. At the same time, costs are piling up—as a consequence of the Network Enforcement Act, Facebook was forced to hire 1,200 moderators.

THE GLOBAL DEBATE ON CONTENT MODERATION

Extensive debates on content moderation are not limited to the EU. The U.S. is increasingly discussing the possibility of modifying Section 230 of the Communications Decency Act, a piece of legislation absolving tech companies of responsibility for regulating what individuals say or do on their platforms. Removing Section 230 would be devastating for social media companies, as moderation costs would skyrocket and the face of the internet as we know it would change. Creativity would likely be the first casualty, as platforms would become extremely cautious about the content shared by their users. As concerns over the behaviour of tech giants become more acute, the Biden administration will likely continue to pressure tech firms to improve their content moderation efforts. A massive federal antitrust lawsuit launched against Facebook in 2020 already threatens the survival of the company in its current form. While the EU pursues its own regulatory strategy, the court battle against Facebook and the potential removal of Section 230 could change the face of American social media companies domestically.

The DMA and the DSA are significant milestones in Europe's commitment to enhance the regulation of digital activities. Even though the European Commission's proposal has not yet become law, it presents the opportunity to debate the role of corporations and governments in the digital frontier. Discussions over digital activities will continue, and the final versions of the DSA and the DMA will emerge by 2023 at the earliest. Implementation into domestic law and the subsequent legal challenges could further delay the adoption of the directives. Regardless, these proposals represent the beginning of a global shift in the way that tech giants are regulated. Growing concern over competition, privacy, and the ability of tech companies to shape our daily lives and even our beliefs are beginning to be met with legislative responses. While the rapid evolution of digital technologies may be exciting, it has dramatically outpaced the development of regulations needed to minimize the negative social impacts that accompany these technologies.



Pierre Miller is a dual degree student pursuing both a Master of Global Affairs at the Munk School of Global Affairs & Public Policy and a Master in Public Policy at Sciences Po. He recently completed an internship with UNESCO New Delhi within the Social and Human Sciences team. Pierre completed his undergraduate degree at Sciences Po, receiving a BA in Political Sciences with an emphasis on History while attending the Sorbonne and receiving a BSc in Physics. He was a visiting student at Johns Hopkins University from 2018 to 2019 and has been involved in several multidisciplinary projects focusing on a wide range of issues from art to climate change. Pierre's main interests are elections, European negotiations, and the implications of global warming.

True or False: Is It Time for International Law to Address Disinformation?

BY FREDERIC COSSETTE | INTERNATIONAL LAW



PHOTO SOURCE: UNSPLASH, MAX MUSELMANN

IN 1971, the U.S. Supreme Court crystallized the power of the press as the “fourth power” in a landmark decision that allowed the New York Times and the Washington Post to publish the classified Pentagon Papers in spite of opposition from the Nixon administration. Not only was the freedom of the press safeguarded, but it was also recognized as the last check and balance that could speak truth to power.

However, this institutionalization of the power of the press is under fire from nationalist governments, a phenomenon facilitated by the proliferation of news sources and the rise of social media. To safeguard democratic institutions, an equilibrium must be struck to preserve the freedom of the press while limiting the disinformation that plagues the news world. States have the legal tools to push back against disinformation within their judiciary systems and there is increasing pressure for tech companies such as Twitter and Facebook to take respon-

sibility for the false content that circulates on their platforms. But what are the legal options when disinformation comes from foreign sources or even foreign states? What can a state do when a disinformation campaign led by a foreign state interferes in its own democratic elections? This is a scenario that is ever more recurrent and for which international law does not have a definitive remedy, even though the interconnectivity of our digital world necessitates a concerted effort to fight back against disinformation.

WHAT IS FAKE NEWS?

The first issue is to differentiate false news from distorted news or, in the words of Kellyanne Conway, “alternative facts.” False news is comprised of false information that is easy to rebuke. Distorted news, however, is harder to counter since it tends to use factual information to paint

an inaccurate picture of reality. For simplification purposes, this article uses the term ‘fake news’ indiscriminately. The second issue is in attributing the origins of the fake news to a foreign state. Some media outlets such as Russia’s RT or Sputnik and China’s China Daily are heavily financed by their respective governments but remain separate legal entities. Another tactic utilized by foreign states entails conducting disinformation campaigns on social media through bots—fake accounts—that spin fake news and spoil debates with inaccurate information. These cyber operations are usually performed by professional hackers hired by the state, which leave no direct trace of state involvement.

However, the presence of fake news attributed to a foreign state would hardly warrant foreign intervention. In international law, the principle of non-intervention protects the sovereignty of the state by forbidding any coercive intervention that would impede on its ability to make its own decisions. But fake news can breach the non-intervention principle if it manipulatively constrains people in the exercise of their free will. In other words, fake news constitutes an interference in a democratic process when it influences people to make different decisions from those they would have made with accurate information. Distorted news cannot however be considered as such because it is not false information, but rather true information manipulated and taken out of its context to create a distorted image of reality. However, it is no less dangerous. In fact, while fake news can be debunked by facts, distorted news requires more nuanced work, as it must be exposed by providing additional context to paint an accurate picture of reality.

INTERNATIONAL LEGAL REMEDIES

Because of its complexity and relative novelty, specialized international law governing cyberspace is still in development. In the absence of such specialized regulation, a patchwork of legal provisions is usually adopted and stretched to account for the technological component of a case. These shortcomings necessitate the creation of specialized law.

In 2017, a group of experts assembled by the NATO Cooperative Cyber Defence Center of Excellence wrote the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. It lists 154 international rules of

customary international law that should be applied to cyber operations. Based on the principle of sovereignty, Rule 66 prohibits the coercive intervention of a state in the internal or external affairs of another, even in cyberspace. The Tallinn Manual, however, is limited in so far as it is customary law, and thus does not create concrete obligations.

Disinformation is not without international legal precedent. In 1936, the International Convention on the Use of Broadcasting in the Cause of Peace was adopted by the League of Nations and is still in force as part of the United Nations’ legal structure. Article 3(1) states: “The High Contracting Parties mutually undertake to prohibit and, if occasion arises, to stop without delay within their respective territories any transmission likely to harm good international understanding by statements the incorrectness of which is or ought to be known to the persons responsible for the broadcast.”

When the USSR ratified the Convention in 1982, they urged states to stand up against the abuse of modern mass media for intervention in the internal affairs of states, for subversive propaganda and for fomenting hostility between peoples.

The convention explicitly forbids false news and is quite comprehensive, with provisions applying to both public

and private broadcasters and establishing a duty of due diligence for broadcasters to “fact-check” the information they diffuse, especially concerning international relations and in times of crisis. In the context of the interwar period, states agreed to limit the interference of broadcasters—deliberate or not—in the conduct of international relations. Only a handful of states are bound by the Convention, including Russia, while the US and China are excluded. When the USSR ratified the Convention in 1982, they urged states to stand up against the abuse of modern mass media for intervention in the internal affairs of states, for subversive propaganda and for fomenting hostility between peoples. This display of good intentions came from a state which controlled all of its domestic media. Only the irony remains today.

BARRIERS TO PROGRESS

The 1936 Convention offers an interesting model for further development in the international regulation of disinformation, though present-day hurdles remain. First, democracies, most notably the United States, will be reluctant to let an international convention interfere with the freedom of speech on their territory. Second, while Russia was the most recent architect of a large-scale election meddling operation during the 2016 U.S. election, the U.S. also has a spotty track record when it comes to interfering in the democratic processes of foreign states. Thus, matters of disinformation and espionage might be better addressed in the realm of diplomacy and surveillance. Third, instead of seeking retaliatory remedies against foreign states, states should look within their own legal system to eliminate the effect of disinformation. This could take the form of an obligation of due diligence imposed on broadcasters and social media platforms.

Yet, while disinformation interference in democratic processes aims at dividing and fragmenting public opinion for political outcomes, one must wonder if traditional national media are not already accomplishing this goal domestically, without the help of any bellicose foreign power. Only by taking the steps necessary to reduce the proliferation of disinformation campaigns will it become apparent whether the resultant socio-political fragmentation is more self-inflicted than otherwise.



Frédéric is a first-year student in the Master of Global Affairs program. He holds a B.Sc. in International Studies and a LL.M. in International Law, both from Université de Montréal. Last year, Frédéric interned at the

Québec Government Office in Munich where he gained invaluable government experience while cultivating his interest for German-speaking countries. In 2017, he also gained NGO experience promoting European institutions through an internship at the Maison de l’Europe de Provence. Frédéric is interested in a wide variety of topics including the law of the sea, questions of sovereignty, Arctic security, the rise of illiberal regimes, global migrations and soft power through sports.

Uber Great, or Great for Uber? Understanding the Future of an Economy Without Employees

BY ALIMAH REHAN | INTERNATIONAL TRADE AND BUSINESS



ELI Lilly, an American pharmaceutical company, was the first in the world to commercially produce insulin, penicillin, and erythromycin—all in a matter of three decades. In 2001, it feared a drop in share prices as its highest revenue generating anti-depressant drug, Prozac, was nearing the date of patent expiration. These fears prompted Eli Lilly to invest in an internet-based, problem-solving platform developed by two of its own employees, which led to the formation of a sub-company, InnoCentive. Eli Lilly went on to invite scientists from around the world to compete online and solve molecular and chemical problems through the InnoCentive website. It awarded only those participants who produced viable marketable solutions, while simultaneously creating a new and free talent pool for the company. The result: successful drugs like Cialis and rising share prices.

InnoCentive was a classic example of how the “gig economy,” based on short-term contracts and independent

workers, established itself in the market. However, global understanding of this type of crowdwork remains limited, and today the term “gig economy” is more often associated with asset-based platform service companies, like Uber or AirBnb.

TYPES OF CROWDWORK

Crowdwork is not simple. It ranges from asset-based services to freelance digital contributions. Professors Debra Howcroft and Birgitta Bergvall-Kåreborn at the University of Manchester and Luleå University of Technology argue that there are at least four types of crowdwork, depending on whether the work is initiated by the “requester” or the worker and the form of remuneration earned (paid, unpaid, or speculative).

While AirBnb, Doordash, and Uber fall under one segment of the gig economy, there are three other distinctive categories. The problem here is that all of these forms of

work are so diverse and wide-ranging that it is difficult to implement uniform policies and regulations.

Types of Remuneration / Initiating Actor	Paid Work	Non-Paid or Speculative Work
Requester Initiated	Type A Online Task Crowdwork (e.g. MTurk, Upwork)	Type B Playbour Crowdwork (e.g. InnoCentive.com, Threadless, TopCoder)
Worker Initiated	Type C Asset-based Services (e.g. AirBnb, Taskrabbit, Uber)	Type D Profession-based Freelance Crowdwork (e.g. iStockphoto, Apple, Google)

Image 2: Typologies of Crowdwork. Adapted from Howcroft and Bergvall-Kåreborn, 2018

WHY INVESTORS LOVE PLATFORMS

Platform-based services that follow the crowdsourcing model have faced criticism since their inception. Investors, however, seem to love these platforms. Notwithstanding the legal and political pressures to regulate them, crowdsourcing offers an ideal business model for investors by featuring low labour costs, short-term hiring of a diverse workforce, huge pools of human capital, minimal investment, scalability, and innovative solutions beyond internal R&D. Some analysts categorise crowdworkers as “working consumers” or passive buyers who become active contributors to a firm’s value chain. This opens avenues for consumer engagement and cheaper market research, especially for fast-moving consumer goods companies (FMCGs) like PepsiCo and Lego. For instance, PepsiCo, the makers of Lays potato chips, used the competition based playbour (Type B) model to attract ideas from their consumers for new flavours of chips. Only one of 3.8 million submissions from the general public won the \$1 million USD inventor prize, thereby saving the company millions in terms of internal R&D that would otherwise have been required to experiment with over three million chip flavours.

Asset-based services, the most controversial and visible of the four typologies in the gig economy, have attracted a lot of public attention despite recent losses in revenue. Market valuations driven by investor enthusiasm are on the rise. Doordash, for example, is valued at \$38 billion USD despite facing losses of \$667 million USD in 2019 and \$149 million USD in the first nine months of 2020. Investors argue that Doordash could easily become a \$500 billion USD plus company, as it has familiarized American customers with the idea of immediacy by fulfilling

orders in less than 25 minutes with just the click of a button. Likewise, market valuations for Uber are growing progressively stronger. Despite losses in ride hailing, the company’s food delivery business has been robust during the pandemic, indicating quick adaptability of offerings based on the assets contributed by workers.

The problem here is that all of these forms of work are so diverse and wide-ranging that it is difficult to implement uniform policies and regulations.

THE CROWDWORKERS

Given the nature of their voluntary participation through platforms with minimal employer obligations, workers in the gig economy are often categorised as “self-employed.” This self-employment comes as a reassurance for crowdworkers who lack access to traditional employee benefits. Many workers rationalize their self-employment in the gig economy by pointing to the greater workplace flexibility, job autonomy, low managerial control, anonymity, and additional income afforded by these positions. Of course, these benefits vary across different types of crowdwork. Looking beyond these personal motivations, we can identify a number of socio-economic compulsions that motivate crowdworkers to fill positions that do not guarantee benefits, employee status, and even pay in some cases. Workers in the gig economy often have traditional jobs and pick platform-based additional tasks to supplement their incomes. A study by Eurofound estimated that more than half of crowdworkers in the UK in 2016 had full time jobs. Within this group, close to 35 per cent earned about half of their income through platform-based work. In an Angus Reid Institute survey

PHOTO SOURCE: FLICKR, DRONEPICR

conducted in Canada last year, 74 per cent of respondents stated that the major benefit of crowdwork was additional income, whereas only 24 per cent said it was job autonomy. For white-collar workers, the industry has presented more opportunities in the post-COVID world. Before the pandemic, there were huge barriers to entry as firms already had full time skilled employees working on location. The basic idea of the gig economy is a shift to a digital marketplace, where a pool of experts from around the world can participate in “free-floating” consulting and other projects through a digital platform. The pandemic has unintentionally pushed workspaces and workers towards “gigification” through the shift to remote work. With work from home becoming the new norm, the only distinction that will remain between full time employees and crowdworkers will be the form of employment contracts signed.

GAPS IN REGULATIONS

The real problem with crowdsourcing is its business model. The industry is based on the notion of voluntary self-employment, task-based pay, and minimal employer liability. Since the original goal of crowdwork was to invite workers without onboarding employees, platform-based companies are obviously wary of responsibility and regulation. Internal regulation at these companies is often managed

The pandemic has unintentionally pushed workspaces and workers towards “gigification” through the shift to remote work.

through a two-way feedback mechanism or digital ratings, which are often limiting. Existing laws are also not far reaching or completely effective. Most crowdworkers

work for multiple platforms at the same time and thus have no single major employer. The 1995 Ontario Labour Relations Act, which extends employee status to dependent workers, fails to guarantee employee status to crowdworkers because they are not tied to any one employer. Legislators have challenged the grey area within which the gig economy functions and demanded the creation of a third class of workers. This is not a straightforward task either. Crowdwork is so diverse that it is difficult to draw a uniform set of policies or regulations that can be applied to all typologies of workers in the system. Despite these challenges, there are still many areas where regulation can and must happen—specifically, in the extension of minimum wage and guaranteed pay, rights to unionise and form cooperatives, and through learning, development and training programs.



Alimah is a second-year Master of Global Affairs Candidate at the Munk School of Global Affairs & Public Policy. She is currently studying the impact of university collaboration on urban innovation as a Research Assistant with Professor Shiri Breznitz and

Professor Shauna Brail. Over the summer of 2020, Alimah worked as a business development intern with the Trade+Impact Association (Africa and North America division). Her research interests include the social shaping of technology, business, and innovations in the developing world.

Technology Alone Cannot Fix Climate Change

BY REEBA KHAN | ENVIRONMENT AND CLIMATE CHANGE



WHILE the COVID-19 pandemic initially reduced global greenhouse gas emissions due to worldwide lockdown measures, the pandemic also revealed a need for stronger climate change policies. Through multiple climate strike marches, activists like Greta Thunberg and ordinary citizens are demanding a greater degree of commitment from governments to ensure climate policies are a priority. Commitment to climate action should be a marriage of government-led public policy initiatives and the mass adoption of effective climate-mitigating technology.

The wonders of our digital world have led to a growing perception that rapid technological advances can provide solutions to a variety of global issues. But across many fields this perception is being contradicted by the reality of the situation, and the climate crisis is no exception. Currently, there is no techno-fix for climate change, which means no technology can serve as a ‘silver bullet’

solution. Furthermore, climate mitigation technology is not being used widely and is still imperfect. However, instead of chasing the development of the perfect technology, the focus should be on making the best of tried and tested technology in combination with public policy which prompts collaboration between the worst polluters.

LIMITATIONS OF A TECHNO-FIX TO CLIMATE CHANGE

Coal and other emission-heavy fossil fuels are prevalent, and mitigating technology has not been scaled to reduce the impact of emissions. Coal consumption spiked between 2000 and 2020, which is concerning because coal is the most polluting fossil fuel and is widely used in Asia and the United States. At first glance, a carbon dioxide

mitigation technology seems to be the solution, but there are several limitations—including the need for the technology to be universally implemented to have a significant impact. Enabling the development of climate mitigation technology becomes even more challenging when pitting economic growth against mitigation.

There are over 400 coal-based power plants in the U.S. alone that emit 1.4 billion metric tons of greenhouse gases annually.

There are over 400 coal-based power plants in the U.S. alone that emit 1.4 billion metric tons of greenhouse gases annually. The emission rates globally are over 35 billion metric tons annually, and substantial mitigation would demand over 100 carbon mitigation projects to eliminate 270 million metric tons of carbon dioxide pollution annually. These estimates were meant to be reached by 2020, however, by the beginning of 2021, there are only 60 such proposed projects, of which only 21 are either operating or being built. Additionally, there are only two coal power plants, Petra Nova in Texas and Kemper in Mississippi, that do not emit carbon dioxide into the atmosphere. While they were met with a lot of fanfare, they represent only 0.5 percent of U.S. coal plants.

Mitigation technology comes with additional challenges, including the fact that the technology itself may contribute to pollution during its construction and depending on its use. In fact, the Petra Nova and Kemper plants mentioned above do not capture all the carbon dioxide from coal—instead, they pump some of it into the ground to extract more oil. This process risks triggering artificial earthquakes from pumping high-pressure liquids into the soil, or even accidentally releasing the trapped carbon dioxide underground. Thus, current mitigation technologies are not a silver bullet as they are neither completely carbon-free, nor are they being utilized widely enough to

have an overall impact.

BETTER TECHNOLOGY IS ON THE HORIZON, BUT HAS NOT MATERIALIZED

While there is an abundance of promising innovation, many technologies are still in their infancy and cannot be replicated outside of the lab. For example, artificial trees are forms of carbon-capture technology that imitate the carbon-storing function of real trees, but they cannot yet be made at a mass scale. Artificial trees could have a significant impact, as one square kilometer of artificial trees could sequester four million tons of carbon annually. While this sounds promising, it would take more than 100 million artificial trees to counterbalance the 40 billion metric tons of carbon dioxide released annually. The cost of installing one artificial tree is \$350,000 USD, which makes it exceedingly difficult and extremely costly to plant a forest, let alone millions of artificial trees. There is not yet a market for such products, and people are hesitant to be the first to pay the price. It would take sizable investments from the likes of Mark Zuckerberg for innovative projects of this nature to take off at the required scale.

THE PATH FORWARD AND THE ROLE OF PUBLIC POLICY

As a result of the more pressing issues that arose during the COVID-19 pandemic, innovative climate change technologies are currently not a political priority. Many countries have eased environmental regulations in order to facilitate financial growth as part of their COVID-19 economic recovery strategies. While there are also economically friendly environmental options available, their benefits are not seen until years down the line and are thus viewed as too costly. During the last financial crisis, U.S. states spent up to 15 per cent of their stimulus package on cleaner energy initiatives, but there is no similar action taking place today.

However, the EU is an exception to the back-peddling trend largely due to the European Green Deal, a \$1.1 trillion deal which features climate-focused infrastructure and a decarbonization plan. There is political and market support for technologies that are practical and effective,

marking a potent case for the marriage of public policy and technology. There is also political will from across the spectrum powering such an ambitious plan, since climate change mitigation has been on the EU's radar for decades. For instance, the three big oil companies—Equinor, Shell, and Total—were backed by support from Norwegian and EU governments for a project called Northern Lights, which aims to establish a network of carbon capture sequestering systems that will capture emissions from areas around the North Sea and inject them underground. While the global trend has been to move away from green goals, the EU government's support has been key and marries well with tried and tested technology.

There is political and market support for technologies that are practical and effective, marking a potent case for the marriage of public policy and technology.

CONCLUSION

In all, a techno-fix alone will not be enough to address climate change. Firstly, current technology is neither flawless nor is it being used at the necessary scale. Secondly, the ideal technology, such as artificial trees, are not currently replicable at a mass scale. Thirdly, the best results are typically seen at the intersection between technology and public policy. Imperfect as the tried and tested technology maybe, it has a better shot of being effective when implemented at a large scale, as the European Green Deal and its cross-industry collaboration makes apparent.



Reeba Khan is a first-year student in the Master of Global Affairs program at the University of Toronto. She plans on studying sustainable development with a specialization in Environmental Studies. Recently, she completed her

Honours Bachelor of Arts with high distinction at the University of Toronto. She double majored in Political Science and Environmental Management. As an undergraduate, she extensively participated in the Research Opportunity Program (ROP). Her projects involved studying the presence of green infrastructure in Toronto and partnering with an Indigenous friendship center in Peel. Additionally, she published an article on environmental regulations through Federalism-E, and she interned for the United Nations Development Program as their research analyst.

A New Way Forward? The Cryptocurrency Revolution in Developing Countries

BY JUN PARK | GLOBAL DEVELOPMENT



THE World Bank estimates that roughly 1.7 billion people worldwide do not have a bank account. The majority of these people are located in developing countries, where financial institutions are weak. The poor performance of these institutions makes it difficult for people to accumulate capital and seek financial assistance, making social mobility much more challenging. However, technological innovations such as cryptocurrencies are becoming increasingly prevalent in these countries, providing financial stability and, ultimately, a chance at a better life.

Cryptocurrencies (CCs) are digital currencies that allow for secure transactions through the use of sophisticated encryption technology, commonly known as cryptography. CCs are denominated in terms of virtual coins (like Bitcoin) or tokens which are represented by ledger entries that are recorded and stored in blockchains. Most CCs record transactions through blockchain technology, which is essentially a digital ledger that is transparent and

unalterable and operates through decentralized networks and encryption technologies. The way in which the popular word processor Google Docs functions presents a clear analogy for blockchains. When a document is created and shared with others, the document is distributed rather than copied or transferred. This creates a decentralized distribution system where everyone is granted access to the document at the same time, with all modifications recorded in real time, allowing for complete transparency. CCs use blockchain technology to ensure that all transactions are secure, transparent, and, most importantly, create a system free from central authority, which theoretically makes them immune from government interference or manipulation.

THE LIMITATIONS OF TRADITIONAL CURRENCIES

The adoption of CCs can be immensely beneficial in developing countries, as they are fast to implement and are financially inclusive by nature. Despite the appeal of CCs, most people still rely on traditional financial institutions. Financial intermediaries are not only vital to individuals but also to companies and businesses, as they are a prominent source of employment for many people. Firms operating in developing countries tend to experience slower growth and fail more often compared to those in developed countries, often due to the lack of available financial resources. This forces many firms to resort to suboptimal behaviours, such as subprime loans or loan sharks. Thus, firms in developing countries are often limited in their ability to generate sufficient revenues and profits, which leads to weaker contributions to the local economy through fewer jobs, lower salaries, and lower tax volumes. When coupled with poorly performing financial institutions and a weak or volatile currency, these outcomes can cripple a country's economy.

Firms operating in developing countries tend to experience slower growth and fail more often compared to those in developed countries, often due to the lack of available financial resources.

For example, Venezuela continues to experience one of the worst financial crises the world has ever seen. While there are a host of explanations for the crisis, poor economic management from the government coupled with rampant corruption have sent the economy into a death spiral. As a result, the country's financial institutions have all but collapsed, rendering the national currency, the bolivar, completely useless with inflation rates exceeding 1,000,000 per cent in 2018. In 2016, one could trade

roughly ten bolivars for one U.S. dollar. In 2021, one U.S. dollar is worth more than 1.76 million bolivars. With financial institutions crippled and the bolivar essentially worthless, the country has experienced a negative development pattern characterized by a dramatic rise in poverty, mass unemployment, stagnation in productive industries, and a dramatic fall in the quality of life.

THE ADVANTAGES OF CRYPTOCURRENCIES

While Venezuela is an extreme example, it demonstrates some of the difficulties that a country can face when financial institutions become weak or dysfunctional. In these circumstances, CCs can be a game changer for many people. Rapid technological advances continue to make the internet more accessible in many parts of the world. In 2019, more than half of the world's population had access to the internet, compared to only 29 per cent in 2010. For Venezuela, CCs continue to provide protection against inflation and opportunities for financial growth for thousands of people. The use of CCs has provided Venezuelans with access to financial resources that previously lay outside their reach, allowing them to sell goods and services and be paid a living wage. For context, the minimum wage in Venezuela is \$2 a month, making many jobs in the country virtually worthless, while those who utilize CCs can make anywhere from \$10 to hundreds of dollars each week. CCs also enable wealth accumulation in developing countries by eliminating costly transaction fees and transfer times. In Haiti, money transfers from expatriate workers make up 26 per cent of Haiti's GDP (roughly \$1.5 billion USD). However, remittance fees can range anywhere from 8-10 per cent of GDP, or \$150 million USD annually. Even in countries like Haiti where internet infrastructure is weak, people are using smartphones to access CCs. In fact, CCs and blockchain technologies are blossoming in the country as more people are adopting cryptocurrencies to avoid government barriers and take more control of their finances.

CCs also have the ability to dramatically reduce corruption and financial mismanagement. The hallmark of CCs is that they are completely transparent and decentralized, meaning that no single person or entity wields disproportionate influence over them. Research from Transparency International demonstrates a strong correlation between

PHOTO SOURCE: FLICKR, OPEN GRID SCHEDULER / GRID ENGINE

corruption and poverty rates, and corruption is estimated to raise the cost of achieving certain UN Millennium Development Goals by as much as \$48 billion USD. While CCs alone are not capable of rooting out corruption, they can serve as a catalyst for systematically reducing corruption. Spending for government or FDI projects can be tracked in real time in order to determine whether or not funds are being used for their intended purpose. Due to their decentralized nature, transaction records would be virtually impossible to alter, as no one actor can unilaterally make changes to the blockchain. According to the Brookings Institution, CCs have the potential to reduce illegal public sector bribes by \$1.5-2 trillion USD annually, which could dramatically accelerate development efforts worldwide.

Spending for government or FDI projects can be tracked in real time in order to determine whether or not funds are being used for their intended purpose.

CHALLENGES AND CONSIDERATIONS MOVING FORWARD

Although CCs have significant potential to help those in developing countries, they are by no means a 'silver bullet' solution. One of the biggest challenges facing CCs is that they are highly volatile. Since there are no central authorities to regulate the performance of CCs, prices tend to fluctuate more frequently compared to traditional national currencies. To limit the fluctuation of prices, many CCs have progressed in the direction of a more formally regulated currency, although this undermines the autonomous aspect of CCs. Despite the rapid global

proliferation of CCs, the technology is still in its infancy. This includes undiscovered technical flaws that could potentially cripple the system with very little notice. It is also important to note that CCs require reliable internet connectivity, which is often an issue in many developing countries.

CCs have revolutionized the way transactions are conducted in digital markets. In developed economies, they have proven to be great sources of investment and a convenient way to conduct secure transactions. Although imperfect, CCs have immense potential to improve financial stability and overall quality of life for citizens of developing nations as well.



Jun Park is a first-year Master of Global Affairs student. He graduated from the University of Western Ontario in 2020 with an Honours Specialization in International Relations. Prior to Munk, Jun worked at Western's political think tank, the Leadership and Democracy

Lab, where he produced articles outlining the challenges facing Puerto Rico's Tourism Industry and worked as a team leader overseeing a client project for Ameresco Energy. In 2018 Jun took part in a community development and conservation project in rural northern Thailand, collaborating with the local population and studying indigenous spices. Jun's main focus of research is on innovation, development and sustainability.



*Join the global conversation.
munkgc.com*