CONCORDIA

HUMAN RIGHTS IN THE DIGITAL AGE

RIGHTS CITY 2021 CONFERENCE REPORT

Université Concordia University

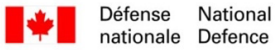
MONTREAL INSTITUTE FOR GENOCIDE AND HUMAN RIGHTS STUDIES

National Defence Défense nationale

Human Rights in the Digital Age

Rights City 2021 Conference Report

Partners



Human Rights in the Digital Age
Rights City 2021 Conference Report

Introduction

The 2021 #RightsCity conference, held online between 15 and 18 June 2021, focused on the intersection of human rights, security and technology. #RightsCity is Canada's leading human rights forum and dialogue. Began in 2017 as a joint initiative between the Montreal Institute for Genocide and Human Rights Studies and the Raoul Wallenberg Centre for Human Rights, the conference is now in its third year. Organised by the Montreal Institute for Genocide and Human Rights Studies at Concordia University, the event was funded by the Canadian Department of National Defence and carried out in partnership with the Raoul Wallenberg Center for Human Rights, the University of Ottawa's Human Rights Research and Education Center, the Embassy of the Kingdom of the Netherlands to Canada, the Global Action Against Mass Atrocity Crimes initiative, the Embassy of the United States to Canada, and under the patronage of the Canadian Commission for UNESCO.

The conference brought together leading global experts working across the governmental, non-governmental and private sectors to consider the threats and opportunities presented by the digital revolution to the respect for and protection of human rights and democratic values.

The panel discussions focused on the following issues:

- Can democracy survive the internet? Foreign interference and disinformation campaigns
- Confronting digital authoritarianism
- The case for a digital Geneva Convention
- Digital attacks on human rights and democracy activists
- Moving to unite democracies on technology
- Social media as a tool to investigate and prosecute atrocity crimes
- Confronting online hate speech

The following paper summarises the major themes of the discussions and puts forward recommendations for advancing human rights and democratic values in the digital age.

Note from the Director

#RightsCity is Canada's leading human rights forum and dialogue. Began in 2017 to coincide with Montreal's 375th anniversary celebrations, the event is a joint initiative between the Montreal Institute for Genocide and Human Rights Studies and the Raoul Wallenberg Centre for Human Rights. Now in its third year, the event was held online in light of the Covid-19 pandemic. Organised by the Montreal Institute for Genocide and Human Rights Studies at Concordia University, the event was funded by the Canadian Department of National Defence and carried out in partnership with the Raoul Wallenberg Center for Human Rights, the University of Ottawa's Human Rights Research and Education Center, the Embassy of the Kingdom of the Netherlands to Canada, the Global Action Against Mass Atrocity Crimes initiative, the Embassy of the United States to Canada, and under the patronage of the Canadian Commission for UNESCO.

Context and opening remarks: The dystopian direction of the cyber revolution

- Irwin Cotler, Founder and Chair of the Roaul Wallenberg Centre for Human Rights
- Jason Munyan, Programme Officer, Office of the Special Advisor to the Secretary-General's Special Envoy on Technology

> "When technology races, the law lags" – Irwin Cotler, Founder and Chair of the Raoul Wallenberg Centre for Human Rights

The internet connects two thirds of humanity to information, economic opportunity and communications platforms. Over the past 15 years, it has dominated social, political and economic change. Reliance on the internet has become even more acute during the global pandemic, providing a lifeline for people across the world to access information about the virus and health measures in place, as well as allowing people to work, study and stay in touch. However, the tech revolution has coincided with a global decline of democracy and open, transparent, civic spaces. The threats to security and human rights that were becoming clear before the pandemic have only been accelerated by this increased dependence.

Irwin Cotler used his opening remarks to outline the chilling dystopian features of the cyber revolution, including:

1. The proliferation of state-sponsored cyber warfare to disrupt critical infrastructure, such as cyber and ransomware attacks, and interfere in domestic political processes like elections
2. The weaponization of social media by global authoritarians to repress dissent, silence critique and spread disinformation at home and abroad
3. The exponential increase in hate speech online – including state-sanctioned incitement to hate and violence – and the impact this has on people's lives offline
4. Threats to democracy in Canada and other democracies through the integration of sophisticated technology into law enforcement agencies in ways that violate domestic and international human rights law

Cotler emphasised that the law was not keeping pace with technological advances, leaving dangerous gaps in the legal protections for human rights both in Canada and abroad.

> "Internet shutdowns have become more sophisticated, lasting longer, affecting more people, and targeting vulnerable groups" - Jason Munyan

Jason Munyan of the United Nations (UN) Office of the Secretary-General's Special Envoy on Technology highlighted the Secretary-General's Roadmap for Digital Cooperation as a response to the growing vulnerability of citizens to invasions of privacy, surveillance technology, harassment, and human rights abuses. The Roadmap calls for member states to put human rights at the centre of regulatory frameworks for the development and use of technologies. It also calls for technology corporations to acknowledge the importance of human rights in the digital space. The UN Human Rights Council has repeatedly affirmed that the rights people hold offline must be the same as those online. However, norms guiding behaviour online have not been fully realised. A recent Joint Statement of nine United Nations Special Rapporteurs affirmed that,

> "States continue to leverage these technologies to muzzle dissent, surveil, and quash online and offline collective action and the tech companies have done too little to avert such abuse

> of human rights. We are deeply concerned that these patterns of abuse, which have further accelerated under the exigencies of the pandemic, will continue and exacerbate inequalities worldwide."[1]

Munyan encouraged UN Member States to work with the international body and other technology stakeholders to "make sure that the technological advances of tomorrow to do not come at the expense of the universal fundamental human rights that we pledge to uphold, promote and defend."

Panel 1: Can democracy survive the internet? Foreign interference and disinformation campaigns

- Rafal Rohozinski, Founder and Principal, SecDev Group (Moderator)
- Emily Dreyfuss, Fellow and Senior Editor, Shorenstein Center on Media, Politics and Public Policy
- Alice Sollmeyer, Executive Director, Defend Democracy
- Sophie Zhang, former Facebook employee and Whistleblower

> "Asking 'Can democracy survive the internet' is like asking 'can the climate survive fossil fuels'… I see many similarities between the big tech lobby and the fossil fuel lobby" – Alice Stollmeyer, Executive Director of Defend Democracy

Rafal Rohozinski began the discussion by outlining how the digital revolution is transforming the social contract between institutions and citizens. Traditional gatekeepers of public opinion and social change, such as family, schools and governments, are being circumvented by direct access to information, conversation and entertainment on social media and – increasingly – interactive gaming. The youthfulness of the internet – with two thirds of users under the age of 35 and half of all users under the age of 25 – melds with this new technology to unleash creativity and question the status quo. Rohozinski said that "the present revolution is likely to redefine our institutions and the processes on which they depend". The absence of accepted norms governing the behaviour of corporations, states and users in cyberspace has resulted in a means for anyone to shape discourse, opinions and influence local democratic choice.

> "Like previous technology revolutions, this revolution is likely to redefine our institutions and the processes on which they depend." - Rafal Rohozinski

The panellists all agreed that democratic governments are being critically undermined by a dis-and misinformation crisis. Access to accurate, timely and relevant information is a fundamental pillar of democracy and citizen engagement needs to be cultivated and tended in order to thrive. And yet, internet platforms, whether they are search engines or social media, are not set up to provide users access to the most reliable and true information. Disinformation online – the spreading of untrue, unauthentic information – is the most pressing issue for the health of democracies. The design of current internet platforms privileges the most popular opinions, rather than the most reliable information, and plays on polarisation and extremes to encourage engagement.

A major challenge for states, corporations and civil society actors in countering disinformation is that there are not currently agreed definitions for the terms to describe the different facets of the problem. Sophie Zhang pointed out that companies such as Facebook face a dual problem of the authenticity

[1] Office of the High Commissioner for Human Rights, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27140&LangID=E

of the messenger and/or the message: inauthentic user accounts, which are easily set up, can disseminate false information. This can then be shared maliciously by other fake user accounts, or by real users with genuine or malicious intentions. The distinction between the source and the content of information is further complicated by the transnational character of user-generated content: disinformation can come from a domestic or foreign source. Participants agreed that foreign interference in western public discourse is vastly lower than generally believed. This overemphasis on foreign interference has caused Western politicians and pundits to overlook the fact that unsavoury political beliefs are most often the product of their own citizens and culture. These views are then instrumentalized by opponents and amplified by paid advocates (trolls) or paid fake user accounts. Zhang noted that "it serves Russia interests to exaggerate the ubiquity of their power and influence online".

To protect democracy, participants underlined the importance of a holistic approach to security and human rights. Encouraging technology companies to actively involve more diverse stakeholders in designing platforms by using a participatory design process was suggested as a necessary shift in approach to halting the internet's current focus on polarising and fragmenting users. Strengthening community guidelines and using open-source coding could also support this. Going further, some participants argued that the capitalist incentives of private companies needed to be curtailed to prevent extreme content prevailing on the internet. Breaking up monopolies and rethinking the economy of successful internet content, such as advertising and page views, could allow space for more ethical alternatives to develop.

Panel 2: Confronting digital authoritarianism

- Michael Petrou, Editor-in-Chief, Open Canada (Moderator)
- Chris Meserole, Research Director, AI and Emerging Tech Initiative and Fellow, Foreign Policy Program at the Brookings Institution
- Sophie Richardson, China Director, Human Rights Watch
- Margaret McCuaig-Johnston, Senior Fellow, University of Ottawa's Institute for Science, Society and Policy

> "It is very important to contemplate how states use this technology in environments where they can't vote a government out, or try to change a law, or even send a letter to a local paper complaining about the uses of this technology" – Sophie Richardson, Human Rights Watch

Authoritarian states have been quick to recognise the potential of digital technology in consolidating their control over citizens. China has harnessed digital tools to obtain a deep insight into public sentiment and behaviour, increasing surveillance over the population and heightening control over dissidents, activists, and minority groups. The treatment of the Uighurs in China's Xinjiang Province has been described as a case of crimes against humanity by Human Rights Watch (HRW). Sophie Richardson outlined some of the tools China is using, such as biometric chipped ID cards, DNA databases, facial recognition and gait recognition software, to scrutinise, control and ultimately detain Uighurs. In one instance, HRW uncovered a surveillance application used by police and security forces whose algorithm aggregated data from various feeds. The algorithm evaluated behaviour types to decide whether an individual is suspicious. This evidence, which included behaviours like using the back or front door of the house or talking to neighbours more often, was then used to put Uighurs in arbitrary detention. This heightened state surveillance is all the more concerning when the state leaves no space for civic engagement and accountability.

Capitalisation on the opportunities presented by technology has also exacerbated existing trends towards authoritarianism in weak democracies and in international institutions. Chinese businesses are investing in exporting their technology abroad guided by geostrategic goals. The Government is willing to subsidise technology to authoritarian states and weak democracies. Panellists agreed that more must be done to counter this destabilizing export strategy. Beyond the export and use of specific technologies, China has been working to undermine international human rights norms and legitimise its approach to technology internationally. For the past decade, China has sought to influence industry standards, business regulations and international norms in favour of authoritarian values. By placing state sovereignty over the internet above accountability and human rights law, Chinese diplomatic engagement on technology internationally can be seen as an attempt to put forward its own views and values as the default for behaviour online. Panellists agreed that democratic states were not advancing the resources necessary to represent democratic values at the relevant international fora, allowing Beijing to make serious inroads on internet governance. Margaret McCuaig-Johnston noted that diplomats, like current Canadian Ambassador to the UN, Bob Rae, have been more outspoken on this matter at the UN Security Council and should continue to do so.

> "Xi Jingping's policy to integrate civilian and military technology development means that Canadian researchers partnering with colleagues in China in areas like AI, nanotechnology, biotech, photonics, quantum computing and advanced materials may not realise that their ideas shared with colleagues may be going out the back door into military applications." - Margaret McCuaig-Johnston.

Equally concerning is the complicity of companies and universities from Western democratic states, like Canada, in state-led repression. McCuaig-Johnston explained that several Canadian universities undertake research in partnership with Chinese technology corporations that are implicated in state repression, including that of the Uighurs. Chinese facial recognition software company SenseTime is partnered with the University of Alberta through a mutual partner, the Hong Kong AI Institute; IFlyTech, which has developed voice recognition and voice pattern databases to support the surveillance and persecution of the Uighurs, has established a research chair at the University of Alberta and at Queens University. McCuaig-Johnston stressed that the reach of the Chinese state is such that we can assume that information held by these companies is being passed on to the Chinese government, with the implicit support of Canadian students and academics. All panellists called for better due diligence and ethical reasoning from Canadian universities in their decision making on partnerships, in addition to the current ongoing reviews of Chinese partnerships by provincial authorities in Alberta and the federal government. McCuaig-Johnston suggested that the Canadian Security Intelligence Service could do more to support universities to develop due diligence criteria to inform decision making.

Western businesses must be aware of the dangers of selling technology to authoritarian regimes like China. Meserole explained that while Canada does have strict export laws for technology with military applications, the dangerous civilian applications of software are not often considered in current export regulations. Meserole suggested that since data and AI are difficult to regulate transnationally, the crux of future regulation should focus on limiting computing power. There are very few countries (US, The Netherlands and Japan) capable of producing the equipment necessary to manufacture computer processors. Targeted sanctions on this equipment could be the way forward for export regulation.

Panel 3: The case for a digital Geneva Convention

- Megan Roberts. Director of Policy Planning, UN Foundation (Moderator)
- Stephane Duguin, CEO, Cyber Peace Institute

- Yves Daccord, Fellow, Berkman Klein Center for Internet and Society, Harvard University, formerly Director General of the International Committee of the Red Cross
- Ana Beduschi, Associate Professor, University of Exeter, Associate Research Fellow, Geneva Academy of International Humanitarian Law and Human Rights

> "There is a problem [in current protections] with implementation and a problem with accountability… I don't see how creating a new instrument of international law would then solve this problem" – Ana Beduschi, University of Exeter and Geneva Academy of International Humanitarian Law and Human Rights

Cyber attacks are vastly underreported, and a majority of attacks take place outside of active conflict zones. They are led by both states and non-state actors, who may have affiliations to certain states. Traditionally protected sectors – such as healthcare – are increasingly under attack from both state and non-state actors. The CyberPeace Institute documented a 45% increase in ransomware attacks on critical healthcare infrastructure during the pandemic, compared to a 20% increase in other sectors during the same period. These attacks usually seek to steal medical data, which has become more valuable than financial data on the black market. Data can also be stolen and then modified to be used to fuel disinformation campaigns. Cyber espionage on healthcare data has also increased, with states seeking to use the information to gain geopolitical influence over a rival.

With such attacks on what are traditionally neutral spaces between states, the international community is working to develop approaches to protecting people from harm on the internet. In 2017 the President of Microsoft, Brad Smith, called for the creation of a new digital Geneva Convention to respond to the challenge of increasing nation-state led cyber attacks. Panellists were skeptical about what a digital Geneva Convention would add to the current protections on human rights without a deeper understanding of the gaps in the available frameworks. Ana Beduschi pointed out that "cyber operations do not occur in a legal vacuum": the existing international frameworks apply to cyberspace. During armed conflict, international humanitarian law applies, while in peacetime, international human rights law takes precedence. The private sector is also expected to adhere to UN guiding principles on business and human rights. The applicability of these mechanisms has been reaffirmed by the United Nations' Open Ended Working Group and the Group of Experts, as well as other parts of the UN's human rights system. Panellists agreed that asking to create a new system of laws to cover online behaviour suggests that the current framework does not work, potentially undermining its legitimacy.

This is not to suggest, however, that the current system is without problems. Panellists all agreed that the most challenging gap in current human rights protections – both online and offline – is that between the protections on paper and their implementation in practice. This gap in accountability is even more stark online since there are not agreed measures of what cyber peace looks like and how often it is violated. Stéphane Duguin described how the CyberPeace Institute documents and measures cyber attacks to understand how people are targeted, what the societal impacts are and how victims can obtain redress, repair, and justice through existing domestic and international legal systems.

The agreement of a new convention would, however, have the benefit of bringing together all actors to define a common framework and grammar for describing human rights threats and protections. Unfortunately, given the current geopolitical climate, panellists were doubtful that states, civil society, private corporations, non state groups, would be able to develop a new convention that would stand

up to current legal standards: the lack of appetite for cooperation globally could lead to an agreement with lower protections. In this climate, the private sector's interest and willingness to discuss how to protect their users from harm online should be encouraged and maintained. All panellists agreed that this willingness should be harnessed to tackle the challenge of implementation of existing frameworks, beginning with increasing transparency about attacks and the mechanisms available to victims for redress, repair and justice.

> "Our compass really should be about people… we are not just trying to manage power dynamics between states… it is about protecting the people affected" - Yves Daccord

Finally, Yves Daccord reflected on the need for humanitarian organisations to shift focus to reflect the need to protect critical infrastructure online, in addition to traditional humanitarian sectors such as healthcare or water, sanitation and hygiene. He put forward the idea of a neutral and impartial area of cyberspace, that states would have to commit to protect without surveillance. Daccord suggested that stakeholders "organise more aggressively around the protection of healthcare" at all times, and in all spheres, offline and online. Panellists stressed that civil society and the private sector should strengthen public awareness of the importance of protecting personal data. They should also provide clearer information on how well the laws are working for victims and how they need to be adjusted to account for digital attacks.

Panel 4: Digital attacks on human rights and democracy activists

- Melody Patry, Advocacy Director, Access Now (Moderator)
- Steven Feldstein, Senior Fellow at Carnegie Endowment, author of the book *Rise of Digital Repression*
- Bethany Allen-Ebrahimian, China Reporter, Axios
- Isabel Linzer, Research Analyst, Technology and Democracy, Freedom House

> "The idea that there is a separation between digital and traditional techniques of oppression is a fiction" – Steven Feldstein

Online oppression has real-world origins. A good predictor of whether a country will use digital tools of oppression against its citizens is if that country is authoritarian or has authoritarian tendencies. Furthermore, the use of tools of online oppression reaches far beyond the sphere of just authoritarian states. Weak democracies are also prone to using technology to erode civic space. India, Brazil, Turkey, the Philippines, Thailand and Ethiopia are all examples in which mass surveillance, high levels of social media scrutiny or disinformation are used by the state to repress dissent. Digital tools are seen by many leaders as a way of extending existing repressive goals. Plus, as AI becomes cheaper, smaller governments, even local police agencies, can buy social media monitoring programmes to find user accounts and root out dissent. Isabel Linzer stated that "the democratisation of this kind of technology is more important than discussing the bespoke spyware products" currently available.

Digital attacks also have real-world consequences. The psychological toll of harassment, as well as increased arrests in response to political, social and religious expression, increased online censorship, and internet shutdowns have an impact on the ability and willingness of activists to continue to speak out. Freedom House's Freedom on the Net report tracks online risks in 65 countries and found that in 2020, online activity led to offline attacks in 32 countries, while government critics and human rights organisations were hacked in response to their work in 38 countries. Intimidation can reach a point where activists retire from public discourse and panellists pointed to examples of trolling campaigns against Uyghur activists. In spite of their vulnerability to online attacks, activists continue to innovate and capitalise on the opportunities provided by tech platforms. One example cited a recent Buzzfeed

investigation, which used censored Baidu maps in China to help identify mass Uighur detention facilities, effectively using censorship as a form of evidence of human rights abuses.

> "If you are abusing the excuse of free speech to keep content up on your platform because you don't want to be legally liable or put resources into getting rid of disinformation...then you are part of the problem" - Bethany Allen-Ebrahimian

Mirroring discussions in earlier panels, panellists highlighted China's role in the proliferation of oppressive technology globally, as well as the complicity of tech corporations based in Western democratic countries. China is codifying its authoritarian practices into law, which makes it difficult for US companies to avoid compliance. Companies that have left the Chinese market because they did not want to comply early in their development, like Google, have explored avenues by which they can re-enter the market through separate interfaces, such a pre-censored search engine. Younger technology companies, like Zoom, have chosen to comply, allowing China to exercise increased extraterritorial governance. Bethany Allen-Ebrahimiam cited the example of the US Department of Justice case at the end of 2020, which found that a Zoom executive shared information about Chinese Zoom users living abroad with the Chinese government and worked to shut down their accounts. Melody Patry noted another trend of offering incentives to corporations to hire local staff when they establish offices abroad. Local staff are then recruited as informants for the state, providing information on dissidents. The safety of local staff is a new risk for corporations calculating how to respond to a government's request for compliance with local laws with authoritarian characteristics.

Panellists suggested that CSOs offer digital hygiene training and provide emergency assistance for at-risk activists to improve protections. Technology companies should invest in and advocate for protecting encrypted communication platforms, as well as taking greater responsibility to prevent their platforms from being explicitly manipulated to repress dissent. Democratic governments should restrict the export of surveillance technology, train law enforcement and diplomatic staff to take complaints seriously and work to hold other governments accountable for their actions

Panel 5: Moving to unite democracies on technology

- Colin Robertson, Vice President and Fellow, Canadian Global Affairs Institute (Moderator)
- Kristin Lord, President and CEO, IREX
- Chris Walker, VP Studies and Analysis, National Endowment for Democracy
- Thorsten Benner, Co-Founder and Director, Global Public Policy Institute

> "Our democracies will not fail because of authoritarian technology, they will fail because technology will be used for authoritarian ends" – Thorsten Benner, Global Governance Policy Institute

In recent remarks at the 2021 Munich Security Conference, President Biden stated that "We must shape the rules that will govern the advance of technology and the norms of behavior in cyberspace, artificial intelligence, biotechnology so that they are used to lift people up, not used to pin them down." Since then, he has indicated that he would like to bring together a summit of democracies, the D10, to discuss threats like technology. Panellists agreed with the thrust of this statement, affirming that democracies need to work to build and enshrine norms in line with democratic values both domestically and internationally. Echoing earlier panel discussions, Kristin Lord highlighted the corrosive influence of disinformation on democracies. Democracies can work at several levels to combat these trends: in international fora, in domestic policy, with civil society organisations and with technology companies.

Internationally, democracies have so-far struggled to build norms around the use of technology that are in line with human rights and democratic values. The panel echoed earlier discussions at #RightsCity on China's diplomatic investment in influencing norms and standards and the need for better implementation of existing standards and laws to protect democratic principles. Chris Walker noted that since we cannot expect authoritarian governments to change, citing his recent report on sharp power, stating that "it is up to the democracies… to stimulate race to the top to make certain that democratic values animate and surround technology both for our own societies' health and for the larger struggle in countries that are deciding what path to take". Panellists agreed that any forthcoming summit for democracies should ensure that there is a collective security mechanism that helps to protect democracies against political coercion from authoritarian states, as well as providing a space for mutual learning and amplifying pro-democracy voices.

Thorsten Benner argued that the fight for democracy will be mainly on a domestic front. He outlined two recommendations. First, that democracies take on a defensive agenda to: ensure that Western companies are not complicit in authoritarian regimes; protect those fleeing authoritarian systems; use technology to uncover repression; and support the litigation of human rights abuses. Second, that democracies lead by example by using technology to support democratic processes rather than weakening them at home.

> "The speed and complexity with which the modern technological resources have hit all of us presents an extraordinary burden for any single citizen to shoulder" - Chris Walker

As such, states should be working to increase resources, knowledge and skills available to citizens. Domestically, democracies could learn from each other, taking the examples of Finland, Ukraine and the UK in particular, who are each implementing a society-wide approach to digital security. Policy should consider how to weed out disinformation in partnership with tech platforms and how to make citizens more resilient to misinformation. Panellists agreed that civil society organisations are a key stakeholder in responding to this threat and need to be included in discussions seeking to shape domestic and international rules. Encouraging civil society to play a more meaningful role as a translator and educator will help share the burden with individual citizens in navigating online disinformation.

Civil society organisations are in need of ongoing support, research and networking opportunities in order to share experience and expertise. This is obviously more challenging in countries with shrinking space for civic engagement. Integrating media literacy in school curricula, while also reaching out to older populations through libraries and other means, such as in Sweden and Ukraine, provides good examples of simple policy changes that have impact. Kristin Lord said that "Where I see some shortfalls is looking beyond schools: young people don't vote as much, young people are a small percentage of the population, young people are less likely to forward disinformation than their older counterparts, and so this is where democracies could compare notes and come up with common strategies. She also noted that North America has few examples of media literacy programming, despite its proven success in contesting disinformation.

> "It's not just about teaching people how to check facts...but it is also about recognising emotional manipulation" - Kristin Lord

Tech companies should be held to account through due diligence requirements under current human rights law. The panel presented a variety of perspectives on just how strong Canada should be in its response to potential security threats from technology sourced from authoritarian states – Chinese or otherwise. Panellists focused on the potential role of China's Huawei in developing Canada's 5G

network. Christopher Walker argued that Canada needs to have confidence in the integrity of its infrastructure. Lord cautioned against trade wars that would cause significant recrimination against western companies wanting to export to authoritarian countries, while Benner argued that a fear of economic retribution should not prevent Canada from having secure infrastructure and upholding its technological sovereignty.

Panel 6: Social media as a tool to investigate and prosecute atrocity crimes

- John Packer, Associate Professor of Law, Director of the Human Rights Research and Education Centre, University of Ottawa (Moderator)
- Nick Waters, Senior Investigator, Bellingcat
- Stephanie Barbour, Senior Advisor on Sexual and Gender Based Violence, Commission for International Justice and Accountability
- Alexa Koenig, Executive Director of the Human Rights Center, UC Berkeley

> "For every physical event that takes place, there is a ripple in the digital world" – Nick Waters, Bellingcat

Smartphone technology and social media are potent tools for bearing witness to atrocity crimes like genocide, war crimes, crimes against humanity and ethnic cleansing. Digital, open-source information to support criminal investigations come in many forms: user-generated content such as video footage and photography, satellite imagery, digital documentation, and physical hardware. With feeds like Twitter updating with 6,000 tweets every second, however, finding relevant information is a huge challenge. Nick Waters pointed out that the data is "ultimately ephemeral - videos get deleted and accounts get removed...but what we have are snapshots and moments of memory of events". He stressed that in this sense, digital open source data can be incredibly important.

The panellists described how organisations like Bellingcat, the Commission for International Justice and Accountability (CIJA) and the Berkeley Centre for Human Rights work to gather, analyse and preserve online evidence so that it can be used in court as evidence in future investigations of atrocity crimes. Stephanie Barbour explained that CIJA has focused on gathering evidence of war crimes, crimes against humanity and genocide in Syria. The Commission uses digital evidence as part of a larger body of evidence that can help to develop case files. Digital evidence can provide clues on what investigations should focus on, help to map out the structure and policies of perpetrating organisations and act as corroborative material to more traditional sources.

Alexa Koenig outlined the work of the Berkeley Centre, which has been advising on standards and protocols for collecting digital evidence in response to the ad hoc approach of judges to allowing this type of evidence in court. The Berkeley Protocol on Digital Open Source Investigations outlines a three-step process for verifying online content and minimising bias. This includes analysis of:

- The technical data attached to the information, such as meta data or exit data behind the footage of photo recording information like the device, date and coordinates
- Sources and reliability, such as analysing who the source is and how consistent this information is with the other content on their timelines
- Content, such as investigating how consistent the evidence is with the known context and triangulating it with other forms of evidence like satellite imagery and witness testimony

The use of open-source data also brings ethical challenges. Often, the original source of the data is not known, nor are the identities of those shown in photos or videos, which makes it difficult to protect privacy and ensure evidence is used consensually. Waters noted that even when the source is not

known, certain content can still be deemed to be in the public interest. Barbour said that CIJA's approach was to take each piece of evidence individually on a case-by-case basis. This was particularly true when it came to documenting proof of atrocity crimes, like sexual and gender based, since victims are in a vulnerable situation and current legal norms do not place an evidentiary burden on victims to prove that sexual violence took place.

> "The contours of practice and law around this are constantly evolving and changing as the materials that we bring before judges are evolving and changing so it is very difficult to predict what the reactions will be." - Stephanie Barbour

Koenig outlined a typology developed by the Berkeley Centre to help investigators work through the issue of consent in digital investigations. This approach has a three-pronged ethics framework to guide investigators in the handling of digital information: consider the legal requirements of consent in each case; consider the professional codes of the individual investigator, whether they be a lawyer or a data analyst or an academic researcher; and the emergent norms and practice in this area, which is split into the physical, digital and psychological security issues implicated by the use of the information, human rights requirements, and the accuracy and quality of the information. This framework can help investigators navigate ethical issues around privacy and consent.

All of the panellists were positive about the admissibility of well-handled information in court and were hopeful for the role digital evidence could have in future prosecutions of atrocity crimes.

Panel 7: Confronting online hate speech

- Naomi Kikoler, Director, Simon-Skjodt Center for the Prevention of Genocide, United States Holocaust Memorial Museum (Moderator)
- Silvia Fernandez, Chair, Global Action Against Mass Atrocity Crimes
- Fernand de Varennes, UN Special Rapporteur for Minorities
- Iain Levine, Senior Human Rights Advisor, Facebook

> "No society is immune to hate speech", Silvia Fernandez, Global Action Against Mass Atrocities

Naomi Kikoler began the discussion by describing the growing recognition of hate speech as a precursor to atrocity crimes. Like traditional communication tools, such as the radio or printed leaflets, social media has shown that it is capable of amplifying intolerance and prejudice to create an environment where hate speech and hate crimes are possible. Fernand de Varennes, UN Special Rapporteur for Minorities, stressed that the main target of hate speech and hate crimes are minority groups. In Sri Lanka, Myanmar, India and elsewhere, online hate against minorities is on the rise and global antisemitism has been found to be increasing. De Varennes stated that "it is hard to claim that technology is a force for good in these conditions, if we allow it to be the medium for evil".

De Varennes called on social media companies to recognise that hate is most frequently targeted against minorities to strengthen their response, such as by providing disaggregated data to allow analysts to better understand who vulnerable groups are and how they can be protected. He also argued that the liability of social media companies for hosting hate propaganda needed to be made clearer, stating that "no business should be immune from the harm that they directly contribute to". A UN report into the violence in Myanmar found that Facebook had been used as a tool to spread hate and incite attacks against the Rohingya minority in 2017. Iain Levine of Facebook admitted that this was a low point for the platform and described Facebook's new approach to human rights. A new human rights policy clarifies the company's responsibilities under the UN Guiding Principles for Business and Human Rights, as well as laying out commitments to international human rights

conventions. The roll out of the policy is complemented by training for content moderators. A major challenge for implementation and enforcement is the scale at which Facebook works; there are over 1.8 billion users, and 100 billion pieces of content are uploaded to the site every day. Levine emphasised Facebook's new approach to Myanmar during the current coup, during which time they have removed the Tatmadaw (the Burmese Army) from the platform, citing responsibilities under the UN Principles for Business and Human Rights.

Despite growing recognition of the problem, research to help understand the processes that lead from discrimination to hate speech to hate crimes lags. There is no agreed definition of hate speech, although it is generally illegal when it directly incites violence. However, the earlier language used to set the scene and legitimise later hate and violence is not currently covered by legal definitions. Panellists agreed that the question of how to define hate speech and its precursors without infringing on freedom of speech is the most pressing question for stakeholders working in this field today.

> "The content removal processes don't always work as well for the minorities as they should… unfortunately, the human content moderators may themselves be bias against these minorities" - Fernand de Varennes

The lack of definition for the space before incitement to violence is a stumbling block for state cooperation on atrocity prevention. Nevertheless, Silvia Fernandez described the efforts of the Global Action Against Mass Atrocities (GAAMAC) network, which works to "cultivate a culture of prevention" among its members. GAAMAC recognises the importance of hate speech as an indicator of potential atrocity crimes and is discussing tools available to respond. The role that education could play in equipping people to identify hate speech requires further research, as does the work of organisations disseminating counter narratives. Ian Levin described how Facebook has developed a partnership with Defy Hate Now in South Sudan, Ethiopia and Cameroon to identify disinformation in local languages on the platform and educate local communities in recognising and countering hate speech.

Another possible response is to repress hate speech. Fernandez stressed that there needs to be a clear definition of hate speech so that repression does not infringe on free speech. All of the panellists underlined the importance of the Rabat Plan of Action, which sets out principles for distinguishing between freedom of expression and incitement to hatred. Panellists agreed that the principles are sorely underused. The Plan of Action outlines a six-part threshold test, which considers: the context, status of the speaker, intent, content, extent of dissemination and likelihood of harm.

At Facebook, content is regulated by Community Standards. In cases where these standards are broken, 97% of content is removed automatically by algorithm. The remaining content flagged as abusive is followed by human content moderators, who make decisions about what is and is not allowed on the site. Levin acknowledged that the company needs to go further than simply removing content to be able to tackle misinformation and disinformation, such as by linking to credible information to promote counter narratives. De Varennes stressed that human moderators needed to be assessed for bias themselves and have training that makes them more sensitive to the specific vulnerabilities of minority groups and the way in which they are targeted online.

However, panellists noted that individual approaches are not enough to combat the threat of hate speech online. States, the private sector and civil society need to agree on a global, legally binding approach that balances free speech with protection against hate speech, establishes liability for social media companies, improves content moderation and commits to protecting minorities. While there is growing political will to address the problem, efforts have not yet transcended national or corporation-level activities. This is all the more important when faced with the spread of

authoritarianism and the use of this debate by authoritarian governments to repress dissent and curb free speech in their own countries and abroad.

Conclusions

The norms, laws and rules that will regulate the behaviour of states, individuals and corporations online are being contested daily. Two camps are bubbling to the surface and a tussle between the use of digital tools for authoritarian and democratic ends has become clearer in the last five years. Until recently, democratic states have been complacent in the face of Chinese investments in influencing the creation of standards for online activities, in tandem with wider efforts to undermine the international human rights system and shrink civic space. Democratic states have been slow to recognise and understand the impact of the way online technology is currently designed and its influence on citizen's access to and engagement with information. Social media technologies influence the practice of politics and the development of policies, amplifying the influence of individuals and issues in a way that has not been possible before. Developments in artificial intelligence provide the means by which states and corporations are able to collate vast reams of data about citizens and users.

These technological advances are taking place faster than governments and civil society can analyse their impacts and agree on safeguards against their abuse. Agreed norms to regulate national and international behaviour online are lagging behind the changes, creating an environment in which the rights of citizens are open to violation. The design of the online world itself, in which simplification, melodrama and polarisation is rewarded, and where access to user's personal data is sold for profit, creates an environment conducive to human rights abuses.

It is crucial to recognise that online behaviour has real world origins and consequences. How states, corporations and individuals approach the design, use and sharing of digital tools aligns with their offline identities, strategies and actions. The human rights protections in place for individuals online should be no less fundamental or accountable online than they are offline. While this paper considers solely online manifestations of human rights abuses, any strategy seeking to protect human rights and democratic values online should be integrated with offline actions.

Recommendations

Internationally, the Government of Canada should:

- Work through all available diplomatic channels to strengthen the implementation of international human rights law and international humanitarian law. At minimum, this should be focused specifically on the protection of healthcare services from physical and digital attacks in conflict and during peacetime.
- Lead and support international efforts to ban intrusive surveillance technology, such as facial recognition.
- Explore the development of a targeted international sanctions regime on the equipment necessary for producing processors in order to limit the repressive capabilities of authoritarian governments.
- Be an active contributor in international discussions and debates on democratic governance online: support the development of a common language and understanding of norms for online behaviour, advocate for better implementation of existing international law, increase awareness and usage of the Rabat Plan of Action, encourage the democratic design of online platforms, strengthen liability for technology companies hosting hate speech and protect privacy and personal data.

Domestically, the Government of Canada should:

- Develop a society-wide action plan with provincial governments to strengthen public resilience to disinformation online, including but not limited to integrating media literacy programming into school curricula.
- Restrict the export of technology that can be used to support state organised repression by considering the potential civilian uses of technology in addition to military uses.
- Protect the security of Canadian infrastructure and institutions by providing more detailed guidance for Canadian firms and institutions on criteria for safe partnerships and importation.
- Offer increased funding to Canadian organisations and academic institutions undertaking research and programming in the sphere of digital technology, its impacts on society, legal implications and applications and increasing protections for citizens and activists online.

Canadian social media and technology companies should:

- Develop clear human rights due diligence policies to guide technology development, use and exports in line with the UN Guiding Principles on Human Rights.
- Invest in and advocate for the protection of data, including protecting encrypted communications platforms.
- Take more responsibility for situations where platforms are being explicitly manipulated for repression or disinformation and make changes that reinforce the security of the Canadian public and global human rights standards.

Canadian universities and research institutes should:

- Develop clear ethical criteria to guide decision making on academic partnerships with entities based in authoritarian states.
- Review current partnerships with entities based in authoritarian states to explore vulnerabilities and the potential for complicity in authoritarian repression or data privacy breaches.

Canadian civil society should:

- Educate the Canadian public about what personal data is and why protecting it is important
- Provide digital hygiene training and emergency assistance for at-risk activists
- Advocate for and develop media literacy programming to help Canadians identify misinformation

Prepared by:

This report was written by Alexandra Buskie, a Consultant, for the Montreal Institute for Genocide and Human Rights Studies at Concordia University.

This conference was funded by the Canadian Department of National Defence