

CIGF

Canadian Internet Governance Forum

Report

November 24th & 25th, 2020



PRESENTING SPONSOR



PLATINUM SPONSOR



GOLD SPONSORS



PARTNER



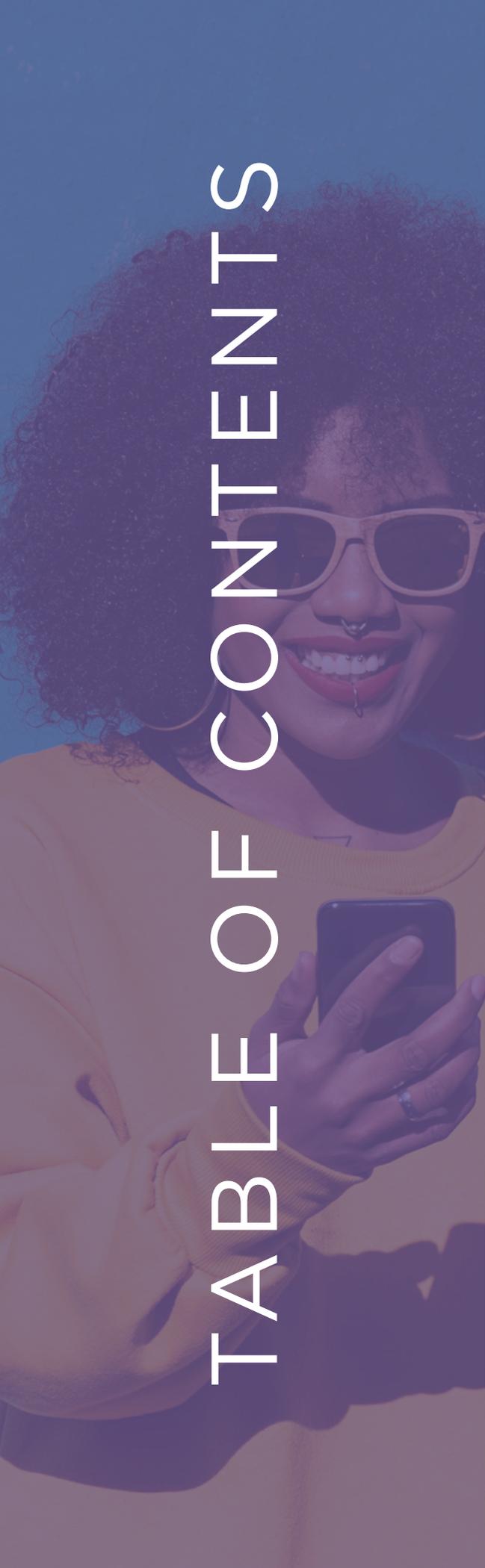


TABLE OF CONTENTS

Executive Summary	3
About CIGF	5
Themes	7
Greetings from the Global IGF and Government of Canada	9
Policing the Conversation? Evaluating Different Approaches to Content Moderation	11
The Internet & COVID-19: How Governments' Backdoor Access Proposals Threaten Canadian Health and Security Online	14
Connecting Indigenous Communities	17
Bonus: Info session on <i>We, the Internet</i>	20
Global Affairs Canada: Freedom Online Coalition	22
Keynote: Canada's Role in the Future of Ethical AI	24
Governing Data and AI in the Public Interest	27
Digital Literacy for the Internet Age	30
Closing Remarks: Byron Holland	33
Info session: An inclusive digital future: What do Canadian and European youth think?	35
Statement of Priorities	37

Executive Summary

On November 24th and 25th, 2020, the Canadian Internet Governance Forum (CIGF) brought together a wide range of stakeholders to engage in a virtual discussion of critical issues impacting the security, safety, privacy, and accessibility of the Canadian internet, as well as potential responses. The 2020 CIGF facilitated an exchange of ideas between top thinkers on topics such as content moderation, digital literacy, data and AI governance, ethical AI, encryption standards, and connectivity challenges in Indigenous communities. It also highlighted examples of public consultation and dialogue on internet governance issues.

This report will provide a statement of priorities for Canadian businesses, governments, civil society groups and end-users involved with internet governance domestically and abroad. It focuses on drawing out the common threads between the insights and recommendations put forward in different sessions.

Inclusion and the multistakeholder approach were among the primary concerns of the organizing committee when addressing the topics discussed at this year's CIGF. Panels were designed to promote a nuanced understanding of each subject and incorporate varied perspectives.

The 2020 CIGF was held at a dynamic time for Canadian internet governance. Bill C-10, An Act to amend the Broadcasting Act, which deals with the issue of Canadian content online, and Bill C-11, the Consumer Privacy Protection Act, were both being debated. In particular, the updates to Canadian legislation and implementation of parts of the Digital Charter promised by Bill C-11 were frequently discussed throughout the 2020 CIGF. Both of these bills demonstrated an elevated willingness to act on internet governance issues by the government. Meanwhile, the lockdowns and social distancing requirements caused by the

pandemic further elevated the role of the internet in Canadians' lives. For many people, this prompted increased scrutiny of their online activity and growing awareness of internet-related issues.

Discussions centered around the themes of trust, data, and the impacts of the COVID-19 pandemic. For stakeholders engaging in internet governance, domestically and abroad, priorities going forward include:

- Using the current window of opportunity to make progress on implementation and standard-setting
- Responding to users' concerns about data collection and usage by strengthening respect for digital rights
- Increasing the accessibility of funding for small organizations working on internet governance issues
- Continuing to develop and promote cooperation across stakeholder groups, particularly when dealing with multi-faceted issues

These priorities are elaborated on in the conclusion of this report.

The event was live streamed, and proceedings, in French and English, can be found on the Canadian IGF Youtube channel.

About the CIGF

The 2020 CIGF builds on the outcomes and lessons of the inaugural 2019 CIGF. It is the result of extensive collaboration between Canadian organizations from civil society, academia, industry, and government. The CIGF is driven by a multistakeholder steering committee, with additional program and sponsorship committees.

Steering Committee members included:

- Chair: Nancy Carter, CANARIE
- Meghan Sali, University of Ottawa
- Allan MacGillivray, CIRA/Secretariat Support
- Franca Pallazo, Internet Society Canada Chapter
- Mark Buell, Internet Society
- Joe Catapano, ICANN
- Katie Watson Jordan, Internet Society
- Michel Lambert, eQualitie (equalit.ie)
- Philippe-Andre Rodriguez, Privy Council Office
- Taylor Bentley, ISED
- Ashleigh Weeden, University of Guelph
- Dr. Catherine Boivie
- Bram Abramson
- Marita Moll, Telecommunities Canada
- Alyssa Moore, CIRA/Secretariat Support
- Josh Tabish, CIRA/Secretariat Support

Program Committee members included:

- Chair: Hosein Badran, Internet Society
- Grace Abuhamad, Element AI
- Emily Fraser, Carleton University
- Matt Hatfield, OpenMedia
- Katie Watson Jordan, Internet Society
- Laura Tribe, OpenMedia
- Taylor Bentley, ISED
- Mariya-Kvitlana Tsap
- Kyle Loree
- Alyssa Moore, CIRA/Secretariat Support
- Josh Tabish, CIRA/Secretariat Support

Sponsorship Committee members included:

- Nancy Carter, CANARIE
- Mark Buell, Internet Society
- Franca Pallazo, Internet Society
Canada Chapter
- Katie Watson Jordan, Internet Society
- Bram Abramson
- Alyssa Moore, CIRA/Secretariat Support
- Josh Tabish, CIRA/Secretariat Support
- Allan MacGillivray,
CIRA/Secretariat Support

The CIGF is recognized as a national IGF initiative by the global Internet Governance Forum, which was established in 2006 by the United Nations as an outcome of the World Summit on the Information Society. The IGF mandate was renewed for an additional ten years by the United Nations General Assembly in 2015.

The event was inclusive and non-commercial in organizational structure and process development. CIGF is a free event, open to all. Due to the COVID-19 pandemic, the 2020 CIGF took place virtually.

Themes

Trust

Discussion about trust cut across several sessions. Perhaps most clearly, misinformation and disinformation erode the concepts of truth and trustworthiness online. Many proposed responses to these issues require placing significant trust in the government or platforms to make decisions about online speech. In this context, digital literacy requires users to exercise skepticism when consuming content online, ensuring that their trust is earned rather than given blindly. Trust is also central to the encryption debate. Strong encryption standards allow users to trust that their privacy and related fundamental rights are not being arbitrarily violated. Finally, establishing trust between different actors and communities is crucial to make progress on complex issues, such as low connectivity in Indigenous and northern communities.

Data

The (mis)use of data was another recurring theme. For example, the policy outcomes of the encryption debate occurring in many western democracies has massive implications for the confidentiality and integrity of personal, professional, and commercial data. Globally, intrusive and non-consensual data collection practices contribute to the rise of digital authoritarianism. Several sessions recognized that the non-rights-respecting use of data is a societal issue, rather than an exclusively personal one. Individuals' data reveals information about other people; this makes it vital to recognize and implement both individual and collective digital rights. It also highlights the importance of enabling meaningful and inclusive public participation in data governance. Public consultations have demonstrated that citizens want to participate and learn more about these issues.

Impacts of the COVID-19 Pandemic

The influence of the COVID-19 pandemic was clear in several of the sessions, as well as the adapted online formats of the CIGF and Global IGF. A consistent refrain was that internet governance issues have become more salient to the public because people have been spending more time online. When users are working, learning, and socializing online, they are likely to become more concerned about the confidentiality and integrity of their data. They have to exercise digital literacy more frequently, whether they are evaluating health information online or simply scrolling through social media. Of course, the increased importance of the internet has deepened the problems faced by those who lack connectivity, particularly in Indigenous and northern communities. Finally, the government has had to develop digital tools, like contact-tracing apps. These tools rely on strong encryption to encourage public trust and can drive collaboration between the government and industry.

Greetings from the Global IGF and Government of Canada

Speakers

- Anriette Esterhuysen, Global IGF
- Paul Charlton, Innovation, Science and Economic Development Canada

Theme(s): Impacts of the COVID-19 Pandemic

Key Issues

- The relationship between the Global IGF and the CIGF
- The Government of Canada's role in internet governance issues
- The importance of the multistakeholder model

Overview of Remarks

The Global Internet Governance Forum has top-down origins, having emerged from the World Summit on the Information Society. National, regional and youth IGF initiatives, like the CIGF, are different because they originated from, and continue to operate in, a more bottom-up manner. This year's Global IGF was also virtual. It was based on four themes: data, environment, trust, and inclusion. The outcomes of the Global IGF and the CIGF should influence each other.

Meanwhile, the Government of Canada is working to advance Canada's vision of an open, resilient, interoperable internet governed according to multistakeholder

principles. It is also mobilizing and investing for connectivity and privacy at the domestic level and recognizes that the importance of internet-related issues has increased due to the pandemic.

Key Insights

- National, regional and youth IGF initiatives, including the CIGF, are significant because they represent the will of people on the ground to collaborate, deliberate, and discuss policy. They ground the global process, but the global process can also guide and inform the NRIs.
- Governments need the input, cooperation, and participation of a wide variety of non-governmental organizations and actors to effectively develop policy related to the internet. This means that the multistakeholder approach is extremely valuable.
- Both the Global IGF and CIGF are examples of the multistakeholder model in action. They include consultation with all stakeholder groups and seek to address the most pressing internet-related issues according to their communities.

Policing the Conversation?

Evaluating Different Approaches to Content Moderation

Panelists

- Suzie Dunn, University of Ottawa
- Steve de Eyre, Tik Tok
- Fenwick McKelvey, Concordia University
- Kevin Chan, Facebook
- David Moscrop, University of Ottawa (moderator)

Theme(s): Trust

Key Issues

- Misinformation and disinformation online
- Hate speech and harmful speech online
- Relationships between online content issues and broader society
- Potential solutions and the complementary roles of government, industry, civil society, and users in developing and implementing them

Discussion Overview

While it is clear that a multistakeholder approach to content moderation is vital, debates around the appropriate roles of certain actors remain.

Governments have a clear role in supporting digital literacy initiatives, education, and public broadcasting. Traditionally, governments have decided on the boundaries of legitimate speech — there is an argument that they should do the same for deceptive or harmful online content, creating a standardized set of rules across platforms.

While the increased involvement of elected officials could improve accountability, this assumes that they are equipped to deal with these issues. Overly strict rules, especially regarding the speed of content removal, can unduly limit expression.

On the other hand, ‘least common denominator’ rules have little potential to affect change.

Platforms can respond to these issues by providing accessible, plain-language community guidelines, incorporating human review when removing content, and notifying users when their posts are taken down, with reference to the community guidelines. However, there are still issues with inconsistent guidelines across platforms, and with enforcing them quickly and at scale. Platforms should be sensitive to the communities and cultures that they create. Furthermore, they should deepen coordination to prevent specific instances of violent or otherwise harmful content from spreading across platforms.

Civil society organizations can play a key role in supporting digital literacy and in amplifying the voices of those who have been impacted by harmful content. They are crucial to ensuring the accountability of other actors.

Users choose which online cultures and communities they want to participate in. They are also responsible for their own speech. However, users who are part of targeted groups cannot fully choose their online environments when harmful content follows them across platforms.

Key Insights

- Conceptual clarity is important, as there are different issues and dynamics surrounding hate speech and harmful speech, or misinformation and disinformation.
- More collaboration and coordination are needed within and across stakeholder groups. The relationships between different platforms, between governments and platforms, and within multistakeholder organizations are particularly important.
- When discussing the roles of government and platforms, there is a tradeoff between accountability and capabilities. While government is accountable to the public through elected officials, platforms have a natural understanding of their own technologies and users.
- There are opportunities to enhance the accountability and transparency of platforms and to improve the capacity of elected officials.
- While these forms of deceptive and harmful content evolve with technological developments, they are often products of deep, structural societal issues. This means that responses require diverse perspectives and areas of expertise.

The Internet & COVID-19: How Governments' Backdoor Access Proposals Threaten Canadian Health and Security Online

Panelists

- Brenda McPhail, Canadian Civil Liberties Association
- Christopher Parsons, Citizen Lab
- Leo Ratledge, Child Rights International Network
- Matt Hatfield, OpenMedia
- Hosein Badran, Internet Society (moderator)

Theme(s): Data, Trust, Impacts of COVID-19

Key Issues

- History of the encryption debate in Canada
- Encryption and COVID-19
- Encryption and human rights
- Encryption, safety, and the human rights of children
- Competing perspectives on encryption

Discussion Overview

Following the first iteration of the encryption debate in the late 1990s, Canada supported the spread of encrypted products, both for commerce and human rights. The increasing prevalence of encryption has tested this position. Over the past two years, the Canadian government's stance on encryption has begun to shift towards ensuring greater access for law enforcement and intelligence agencies under certain circumstances. This is consistent with similar debates occurring in Europe and the United States.

The COVID-19 pandemic has increased the salience of this debate. It has made digital technologies even more necessary for work, education, and accessing services, prompting many users to pay more attention to the security of their data. Furthermore, tools like contact-tracing apps and digital immunity certificates require strong encryption, both for security and to encourage public trust and buy-in. Finally, children are also online more often, intensifying debates around encryption and child safety.

During and beyond the pandemic, strong encryption is essential for the realization of fundamental rights. Freedom of speech, expression, association, religion, and equality rights require access to unmonitored communications to be fully realized. Encryption protects the confidentiality and integrity of communications, preventing the chilling effect of being monitored.

The encryption debate is often framed as a conflict between security and privacy. Perhaps a more nuanced view is there is tension between two types of security: national security and the security of our online personal and professional lives. An important consideration is that any lawful access system would be an extremely valuable target for bad actors, creating a new source of insecurity

Key Insights

- It is vital to actively recognize the connection between privacy and a diverse array of other fundamental rights. This is particularly important because public discourse often subordinates privacy to a vision of public safety that privileges law enforcement over other human activities, as well as simple convenience.
- Policing powers must conform to fundamental rights, including privacy of communications. Encryption provides a layer of technical 'friction', making surveillance more costly and helping to prevent government overstep.
- The COVID-19 pandemic may provide an opportunity for those advocating for strong encryption. The public is more aware of the issue, and the government has relied heavily on public trust to encourage compliance with measures. For purpose-built digital tools, encryption is essential to generating that trust.
- The encryption debate is subject to oversimplification and inaccurate framing, particularly relating to national security and children's interactions with the online world. This represents an area for education and advocacy.

Connecting Indigenous Communities

Panelists

- John Kealoha Garcia, Nation of Hawaii
- Melanie Pilon, Township of Dubreuilville
- Michael Furdyk, TakingITGlobal
- Tim Whiteduck, Technology for the First Nations Education Council
- Mark Buell, Internet Society (moderator)

Theme(s): Trust, Impacts of COVID-19

Key Issues

- Need for increased connectivity in Indigenous and northern communities
- Challenges and opportunities of community broadband
- Training programs and regional technology consortiums
- Importance of partnerships and funding

Discussion Overview

Internet access is a necessity for economic development and the provision of basic services. Of course, the COVID-19 pandemic has only increased its importance — work, education, and much of daily life now take place online. In Canada, Indigenous and northern communities

face significant struggles when it comes to connectivity. They have a real need for accessible, affordable, and reliable broadband.

Attempts to increase connectivity in these communities face significant challenges. First, it is extremely difficult to attract traditional ISPs because small populations are spread out across vast areas. Furthermore, Indigenous and northern communities frequently contend with resource constraints and a lack of technical expertise. Device availability can also pose problems, especially among students.

For many communities, community broadband represents the best means of increasing connectivity. Of course, community broadband projects come with their own challenges. They are very expensive, and the external funding required is often confusing to navigate and difficult to obtain. Funding is also frequently oriented towards larger, traditional ISP projects. Furthermore, because these networks typically include multiple municipalities and First Nations, jurisdictional questions can cause problems for funding, ownership, and security.

Other helpful programs may provide students in these communities with devices and prerecorded educational content. Training in digital literacy and other digital skills is also vital. Finally, regional technology centers and consortiums could help alleviate the resource and knowledge constraints in these communities, though they would require consistent funding.

Key Insights

- For any of the above potential solutions, partnerships are key. These include partnerships between different municipalities and First Nations, as well as those between communities and external actors, like governments and non-profits. In both cases, building trust and developing relationships is paramount. Often, this is easier to do face-to-face, meaning that the COVID-19 pandemic introduces additional difficulties.

- Funding is also essential, considering the resource constraints faced by these communities and the expenses associated with potential solutions. Funding opportunities should be more consistent, streamlined, nimble, and accessible to under-resourced organizations. They should also be less skewed towards traditional ISPs and large, shovel-ready projects.
- Benefits of increased connectivity in Indigenous and northern communities include economic development, more accessible and effective public services, the development of digital literacy, the opportunity to create online content, healthier and more connected communities, and progress towards justice and self-determination.

Bonus: Info session on *We, the Internet*

Speakers

- Michel Lambert, equalit.ie
- Deirdre Collings, SecDev Foundation

Theme(s): Trust, Data, Impacts of COVID-19

Key Issues

- Public consultation and global dialogue on the future of the internet
- Users' thoughts towards the internet, their data, disinformation, and AI
- The importance of enabling public participation in these issues

Overview of Discussion

We the Internet is a global consultation on the future of the internet that began in 2018 and continued until 2020. It aims to better understand who users are, what they are interested in, and what issues they are concerned about. Roughly 5,000 users from over 70 countries, including Canada, participated. This gave Canadians an opportunity to both reflect on and become better informed about internet issues. Due to the pandemic, the consultation had to be moved online in a timely manner.

The consultations included four sessions. First, "The Internet and Me" asked participants about their overall sentiments towards the internet, as well as the impacts of the pandemic on their online behaviour. The second session, "My Digital Data", gave participants a chance

to discuss their concerns about how their data is used, think about how they perceive data, and reflect on their sharing habits. Disinformation was the topic of the third session, with participants discussing their experiences with online disinformation and possible responses to this phenomenon. Finally, the fourth session encouraged participants to share their thoughts on the opportunities and threats associated with AI.

While it is unclear whether there will be a follow-up to We, the Internet, it is apparent that users are interested in these issues. Although participants had varying levels of pre-existing knowledge, they were eager to learn more.

Key Insights

- When discussing their data, participants were highly concerned about a perceived lack of transparency, control, and trust. They tended to view data in terms of human rights, and approximately 50% stated that they would share less data going forward.
- On disinformation, participants favoured a government-led approach and exhibited skepticism towards the involvement of private companies. They thought that education and digital literacy were the strongest tools with which to respond to disinformation.
- The majority of participants felt that they had learned a lot throughout the process. While some people were very well-informed, many were concerned about their lack of knowledge and wanted to learn more. Continued public engagement would help inform people and allow them to express their views.

Global Affairs Canada: Freedom Online Coalition

Speaker: Philippe-André Rodriguez, Global Affairs Canada

Theme(s): Data

Key Issues

- AI and human rights
- Digital authoritarianism
- Canada's involvement in the Freedom Online Coalition

Overview of Remarks

Ensuring that government and industry approaches to the development and governance of emerging technologies uphold Canadian values, such as gender equality, diversity, and inclusion, is a foreign policy priority at Global Affairs Canada. Canada advances this position within the G7, G20, UN, OECD, and other international forums.

Canada helped to found the Freedom Online Coalition 10 years ago. The Coalition is united by the principle that the human rights that people have offline must be respected online. It advocates for a rights-respecting approach to technology in various international forums. A key aspect of the Coalition is its inclusion of stakeholders outside of government, such as academia, the private sector, and civil society. The Coalition's latest joint statement on AI, human rights, and digital authoritarianism is the result of ongoing Canadian leadership and cooperation.

Key Insights

- There are legitimate and serious risks to human rights associated with the development and use of AI in certain contexts. In authoritarian regimes, it can help scale up existing rights violations.
- Biometrics, facial recognition, and other technologies are being used without consent or notice, in ways that violate freedom of association, belief, religion, assembly, association, and liberty of movement.
- Authoritarian regimes are forcing platforms to use automatic content moderation to quell dissent more easily. This is contributing to violations of freedom of expression.
- Canada launched a task force on human rights and AI within the Freedom Online Coalition. After consultation with global experts, this resulted in a joint statement outlining a whole of government/society, multistakeholder approach to AI governance. This approach carefully considers human rights and international law.

Keynote: Canada's Role in the Future of Ethical AI

Speaker: Mark Surman, Mozilla Foundation

Theme(s): Data

Key Issues

- AI in our everyday lives
- Potential for Canadian leadership
- Proposed Consumer Privacy Protection Act: strong points and areas for improvement
- Digital rights, both individual and collective

Overview of Remarks

When we think of ethical AI, we often focus on the ways that these technologies may be misused by governments and militaries, and particularly by authoritarian regimes. While these are very real issues, they can overshadow the subtler ways that concerns around ethics and AI impact our everyday lives. Our smartphones, smart home devices, and social media feeds are all driven by automation and by our data. We are the fuel content we see to whether we can obtain a loan. This means that we have a direct interest in the ethics of AI.

Now could be the time for Canada to take on a larger role in the development of ethical AI. The governance of AI fits into broader questions of internet governance, which governments around the world have become more serious about. Canada's history of visionary thinkers

about technology, values, and communications policy can be a source of inspiration. However, it has been decades since Canada has put forward an ambitious policy that elucidates what we believe in, how communications technology affects society, and how we want to build a policy environment that reflects our shared principles.

The proposed Consumer Privacy Protection Act may represent a step towards renewed Canadian leadership in this area. It would begin to implement the Digital Charter — although this document sets out values to guide the development of Canada’s digital policy, it is non-binding and rather abstract on its own. On the other hand, the Consumer Privacy Protection Act is more concrete and includes strong accountability and enforcement mechanisms.

The Act does prompt some questions about the provision of resources necessary to deal with a high volume of privacy complaints, and there may be some confusion of authority among the proposed enforcement bodies. A potentially more serious issue is that it does not recognize the collective nature of digital rights. Because information about individuals is frequently gleaned from others’ data, many digital rights have a strong collective element.

Key Insights

- Mechanisms for collective action to assert digital rights, such as non-profit cooperatives or data trusts, are important for several reasons. They recognize the collective nature of many digital rights. From a practical standpoint, they increase the likelihood that user’s concerns will be heard and impact the system. This empowers users, pushing back against the imbalance of power that favours security services and corporations.
- While Canada’s Digital Charter was a welcome first step in recognizing the existence of digital rights and setting out the values that should drive digital policy, it was firmly in the

realm of ideas. Legislation that contributes to its implementation, such as the proposed Consumer Privacy Protection Act, is essential for people to be able to exercise these rights in their daily lives.

- Canada has the potential to take on a leadership role in ethical AI and related issues. However, this requires that we continue to translate our values into concrete policies that have a meaningful impact on people's lives. It also requires innovation — fully recognizing the collective elements of digital rights would be a meaningful improvement on similar initiatives in other jurisdictions.
- Key principles for rights-respecting technology include control and consent by the user; transparency, portability, and interoperability; and strong enforcement and accountability. The implementation of these principles would give users more choice about what happens to their data, a greater ability to move to new platforms, and practical means to remedy violations of their digital rights.

Governing Data and AI in the Public Interest

Panelists

- Phil Dawson, Element AI
- Ashley Casovan, AI Global
- Stephen Ibaraki, REDDS Capital
- Skaidra Puodziunas, Ontario Digital Service (moderator)

Theme(s): Data, Impacts of COVID-19

Key Issues

- Data and AI governance
- Partnerships between different stakeholder groups
- Operationalizing ideas and values
- Opportunities and challenges for public participation

Discussion Overview

Coalition-building, developing partnerships within and across stakeholder groups, and creating communities of practice are crucial to advancing data and AI governance in the public interest. Canada's AI institutes — Mila, the Vector Institute, and Amii — are promising examples of collaborative research and development.

The Canadian government has also started to work with industry partners in this area. For instance, the development of the COVID-19 alert app involved close collaboration with an external advisory council. Another example is the Advisory Council on Artificial Intelligence, which includes representatives from industry, academia, and government.

The development of industry standards, roadmaps, and policies dealing with processes, operationalization, and implementation is another crucial element of data and AI governance in the public interest. In Canada, a roadmap of data governance priorities is being developed to further implement the principles of the Digital Charter. This will be consistent with similar instruments in the EU, Australia, and Singapore.

Finally, enabling public participation in data and AI governance helps ensure that all user's interests are considered. Public consultation processes are one way to encourage public involvement. Open government initiatives, which encourage citizens to access, analyze, and contribute to government data and participate in decision-making are also beneficial.

Key Insights

- To reflect the public interest, data and AI governance should draw on the perspectives and expertise of multistakeholder bodies and partnerships.
- It is vital that we move beyond broad statements of values and abstract ideas to the stage of implementation, operationalization, and standard-setting. Canada has made some progress in stage, but we should continue moving forward. This reflects very similar points in the keynote.

- In Canada, there are fewer formal opportunities for public dialogue at the federal level of government compared to the municipal level, which presents a challenge for open government and public participation initiatives.
- Formal mechanisms for participation are necessary but not sufficient to ensure a high level of public participation in data and AI governance. If people are kept out by time commitments and low digital literacy, data and algorithms can reinforce societal issues.

Digital Literacy for the Internet Age

Panelists

- Daphnee Nostrome, Ontario Digital Service
- Lequanne Collins-Bacchus, Treasury Board of Canada Secretariat
- Matthew Johnson, MediaSmarts
- Maureen James, CIRA
- Jim Ghadbane, CANARIE (moderator)

Theme(s): Trust, Impacts of COVID-19

Key Issues

- Defining digital literacy
- The importance of digital literacy
- The state of digital literacy in Canada
- Opportunities and challenges for improving digital literacy

Overview of Discussion

Digital literacy is an extension of media literacy — the ability to access, analyze, evaluate, and produce media. It must consider the interactive nature of digital media, which is largely absent in more traditional formats. The interactivity of digital media has new implications for ethics, privacy, and civic engagement.

Assessing the state of digital literacy in Canada is challenging because there is no comprehensive national-level research on the topic. This is largely because digital literacy is so intimately linked with education, which is a provincial responsibility. Both governments and citizens seem to be asking questions that indicate more awareness of the issue, but data is difficult to come by.

There are several opportunities to improve digital literacy in Canada. Although not without challenges, integrating digital literacy into k-12 curricula is a promising way to reach youth. Outside of the school systems, small initiatives that consider the needs of specific communities have found success. These may be tailored to youth, seniors, new Canadians, remote, northern, and Indigenous communities, or other groups. Clear public awareness campaigns with simple, direct, and concrete calls to action have also been effective.

However, there are also significant challenges. Navigating and obtaining funding for projects is difficult, especially for smaller, community-based initiatives. There are also no uniform, ready-made systems to develop digital literacy in adults. Finally, national coordination is lacking. These all represent potential areas for improvement.

Key Insights

- Digital literacy is a foundational skill that is connected to many of the other issues discussed throughout CIGF 2020. It allows people to exercise their digital rights and identify online misinformation and disinformation. It is also closely related to connectivity issues in Indigenous and northern communities. Given how much of our information comes from online platforms, digital literacy is crucial to ensure people can themselves safe in situations like the COVID-19 pandemic.

- Despite the importance of digital literacy and its relationships with other salient problems, national research, coordination, and leadership in this area is underdeveloped. The number of funding opportunities cannot meet the demand for funding, and many organizations struggle to navigate the system.
- Several civil society organizations have made a positive impact on digital literacy through their projects. Promising approaches to researching, improving, and raising awareness of digital literacy exist in Canada — with more resources and coordination, these could be expanded on.

Closing Remarks: Byron Holland

Speaker: Byron Holland

Key Issues

- The multistakeholder model and the CIGF's role
- Bills C-10, C-11, and the Universal Broadband Fund
- Social upheaval and the limits of freedom of expression online

Overview of Remarks

The multistakeholder model of internet governance, with its inclusion of diverse perspectives, is essential for the internet to meet the needs of users and providers and ensure its safe, secure, and stable operation.

This is particularly important because the Canadian government is debating Bill C-10, which could obligate platforms to produce Canadian content and Bill C-11, the updated privacy legislation. It has also recently unveiled a universal broadband fund. The CIGF allows us to discuss important issues like these.

Key Insights

- Hate, state-sanctioned violence, and extremism are all issues that are increasingly played out in the online world. What happens when the free expression of some is used to systematically suppress the free expression of others? This was not the intent of the people who built and operate the internet.
- NRIs like the CIGF can play an important role in developing principles for the internet to be a force for good. They could form the basis for the responsible regulation for and of the internet, especially if they can be integrated into multistakeholder and multilateral processes at the global level.

Info session: An inclusive digital future: What do Canadian and European youth think?

Speakers

- Katja Melzer, Goethe-Institut
- Antoine Rayroux, Goethe-Institut

Theme(s): Trust, Data

Key Issues

Overview of Discussion

For the past year, a European Union-funded project on transatlantic civil society dialogue has brought together dozens of Canadian and European youth to discuss the future of digital inclusion. It has enabled them to connect, exchange ideas, communicate their concerns, derive policy recommendations and get involved in policymaking processes.

The project brought involved working group sessions of 10-12 young adults in Canadian and European cities. Some sessions were on-site, while others were online. The step-by-step process narrowed down initial ideas to develop specific recommendations while fostering an inclusive and collective way of thinking.

Key Insights

- Digital literacy and education were very important issues for the participants, who were particularly interested in the socioeconomic and civic aspects of these issues. They recommended an increased focus on after-school and after-work programs, in cooperation with community organizations and other actors.
- Another key concern was accessibility, especially in terms of costs to users. Participants advocated for rebates and other ways to bring prices down.
- Young Canadian participants were inspired by European data privacy regulations. They expressed that it is time to implement the Digital Charter. Specific issues of interest included a Canadian equivalent to the right to be forgotten, users' digital footprint after death, and regulations regarding the use and sale of data.
- Overall, there were many similarities among the Canadian and European participants. Both groups were able to learn from each other.

Statement of Priorities

Priority 1: There is a window of opportunity for action on internet governance issues — use it to make progress on implementation and standard-setting.

Many of the issues discussed finally have tabled legislation and a bill number associated with them. The Consumer Privacy Protection Act is a prime example. Furthermore, the elevated importance of the internet throughout the COVID-19 pandemic has also boosted public awareness of these issues. It is vital that we make the most of this opportunity and continue to build on the progress achieved thus far.

In particular, the speakers consistently emphasized the importance of concrete policies and solutions that impact people's lives. Abstract, non-binding documents like the Digital Charter are valuable, but at this stage we should focus on operationalizing those ideas and principles. The Consumer Privacy Protection Act contributes to this goal, and we should continue moving forward while these issues are at the top of the agenda.

Priority 2: Respond to users' concerns about data collection and usage by strengthening respect for digital rights.

Increasingly, Canadians perceive a lack of transparency, control, and trust when it comes to the collection and use of their data. The majority are in favour of applying a human rights perspective to data collection and usage. Moreover, Canadian youth tend to support policies that take inspiration from European data privacy regulations, such as the right to be forgotten. While education and other formal and informal barriers to participation remain a real problem, users are demonstrating that they want to be involved in these conversations.

The implementation of key principles for rights-respecting technology — including control and consent by the user, transparency, portability, and interoperability, and strong enforcement and accountability — could be an effective means of responding to their concerns.

Priority 3: Increase the accessibility of funding for small organizations working on internet governance issues.

In many cases, important initiatives to address issues like connectivity in Indigenous and Northern communities or digital literacy among different groups are carried out by small, community-based organizations. These organizations often face daunting resource constraints and have difficulty navigating the complex funding landscape.

Increasing the amount of funding available is extremely important, but it is only one part of the solution. To make funding more accessible to under-resourced organizations, another goal should be to ensure that opportunities are streamlined, consistent with one another, and less biased towards large projects. Often, these small, community-based organizations make an outsized impact on people's lives. Ensuring that they can access vital resources is crucial for continued progress.

Priority 4: Continue to develop and promote cooperation across stakeholder groups, particularly when dealing with multi-faceted issues.

Finally, many speakers emphasized the importance of a continued multistakeholder approach to internet governance. Policies addressing these issues would require the input, cooperation,

and participation of a wide variety of actors to operate effectively and reflect the public interest. In some areas, more collaboration and coordination within and across stakeholder groups would be beneficial.

This is especially true when it comes to issues that straddle the online and offline worlds.

For example, several speakers pointed out that the misuse of AI, low levels of digital literacy, misinformation,

disinformation, and hateful or extremist online content are often connected to structural problems in society. These and other complex, multi-faceted issues demand a range of diverse perspectives, backgrounds, and areas of expertise. In this context, the multistakeholder approach becomes even more valuable.