CIGF

Canadian Internet Governance Forum

Report

27 February 2019 / Toronto, ON

PRESENTING SPONSOR

cira

PLATINUM SPONSOR

Microsoft

GOLD SPONSORS

Internet Society

canarie

TABLE OF CONTENTS

CIGF

Executive Summary 3

About the Canadian Internet Governance Forum 6

Welcoming Address: Byron Holland, President & CEO, Canadian Internet Registry Authority 8

Opening Keynote Address: Elliot Noss, President & CEO Tucows 11

Considerations for Effective Internet of Things Labels 14

Misinformation, Bots, and Democracy 17

Privacy and Surveillance in the Internet Age 20

Cybersecurity Challenges for Canadian Businesses 23

Are we Building a More Equitable and Inclusive Future? 26

Canada's Role in the Future of Internet Governance 28

Statement of Priorities 31

Executive Summary

On February 27th, 2019, the inaugural Canadian Internet Governance Forum (CIGF) brought together various stakeholders for a national discussion on critical issues affecting access to, and the safety, privacy and security of, the Canadian internet. Now more than ever, cybersecurity and data privacy concerns underpin every aspect of our digital lives. This year's Canadian IGF brought together some of Canada's top thinkers to discuss how privacy, security, artificial intelligence, smart cities, and the Internet of Things (IoT) intersect with one another. It examined the impact on businesses, and the role youth can play in the evolution of the internet.

This report provides a statement of priorities for Canadian businesses, government, and end-users involved with internet governance domestically and abroad. The document focuses on finding common ground underpinned by Canadian values, and also outlines considerations for the Canadian IGF and mechanisms for ongoing collaboration of the Canadian internet community.

The organizing committee emphasized an inclusive, multistakeholder approach to each of the topics addressed at the CIGF. Panels were organized to offer a nuanced view of each subject in order to encourage dialogue. These procedural elements ensured that Canadian values, such as inclusion, global cooperation, peace, and public safety were reflected in the program.

The context of this report is changing user expectations with regard to the internet. For many years, the internet's contribution to social and economic innovation has been the focus. And because of the internet's unprecedented contribution to flourishing businesses, social connections, and knowledge sharing, the online world has remained mostly unregulated.

The digital economy is evolving to be more data-driven and users are becoming increasingly sensitive to the privacy and security issues associated with these models. High profile cases of data privacy concerns, including the relationship between Cambridge Analytica and Facebook or Sidewalk Labs presence in Toronto are top of mind. Major security events like the 2016 Dyn DDoS attack are also worrying. These problems have caused some stakeholders to rethink the role of regulation with respect to activities on the internet.

The scope of issues is growing, as is the pool of stakeholders participating in the conversations. Fortunately, this creates the opportunity for new collaboration and creative solutions in the space. Canadian stakeholders are well positioned to be leaders in addressing the transnational issues associated with the online world and it is important that our unique voice is represented in the global dialogue.

For example, during the debate on privacy and surveillance, speakers highlighted Canada's intermediate position between the European and U.S. approaches to data privacy regulation. In addition, the experience and constraints of small business and innovation in Canada were considered to be essential to approaching issues of cybersecurity. Furthermore, it was generally agreed that inclusivity, including bringing in the perspective of youth, should be included at the outset when addressing internet governance challenges.

Throughout the discussions, several common themes emerged across subject areas. These included trends towards increased regulation; the necessity for plain language content; and, the need for education and digital literacy. For stakeholders engaging in Internet governance domestically and abroad, priorities going forward include the need for:

- A transnational, multistakeholder approach to internet governance.
- Awareness of/education on the issues, and how users can participate in discussions related to internet governance.
- Solutions developed by any stakeholder group that are thoughtful, evidence-based, and proportionate.
- Transparency from both governments and businesses in order to promote public trust and build the capacity of users.

These priorities are elaborated in the conclusion of this report.

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

About the Canadian Internet Governance Forum

The Canadian Internet Governance Forum represents an unprecedented level of collaboration between Canadian organizations from civil society, academia, industry, and government. Steering Committee members included:

Chair:

- Nancy Carter, CANARIE

Committee members:

- Taylor Bentley, Innovation, Science and Economic Development (ISED) Canada
- David Fewer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC) at the Centre for Law, Technology and Society, University of Ottawa
- Sarah Ingle, Youth IGF Canada
- Michel Lambert, Alternatives
- Allan MacGillivray, Canadian Internet Registration Authority (CIRA)
- Pam Miller, Innovation, Science and Economic Development (ISED) Canada
- Marita Moll, Telecommunities Canada
- Alyssa Moore, Canadian Internet Registration Authority (CIRA)
- Tanya O'Callaghan, Canadian Internet Registration Authority (CIRA)
- Franca Palazzo, Internet Society Canada Chapter
- Arjun Sanya, Youth IGF Canada
- Katie Watson Jordan, Internet Society

Nancy E. Carter
Chief Financial Officer of CANARIE

The CIGF is driven by a multistakeholder steering committee and is recognized as a national IGF initiative by the global Internet Governance Forum, which was established in 2006 by 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.

Welcoming Address: Byron Holland, President & CEO, Canadian Internet Registration Authority

Key Issues

- Inconsistent regulation.
- Different approaches to internet governance such as "California-driven" versus European (e.g. General Data Protection Regime).
- Rise of bad actors.
- Public desire for privacy and security versus risky online behaviour.
- Access to high-speed internet crucial for economic growth.
- Concern about misinformation.

Overview of Remarks

The internet has revolutionized how we learn, shop, and interact with each other. As a global resource, however, it is not administered consistently. In the West there is an open industry-driven internet, in contrast to the command-and-control type of approach to regulation in authoritarian regimes. Even in the West, there are inconsistencies (e.g. the venture capital "California-driven" internet versus the privacy-regulated European internet with its General Data Protection Regime (GDPR)). These global discrepancies and activities have repercussions closer to home. They affect the safety and security of Canadians online today, and the future of the internet.

Byron Holland
President and CEO of the Canadian Internet Registration Authority

For the most part, the internet has been a powerful force for good over the last 20 years. It has contributed to flourishing businesses, social connections, and knowledge sharing. The impact of various bad actors, however, is cause for concern. Given this reality, those who have historically been opposed to regulating the internet are reconsidering their position.

According to CIRA's research (conducted in December 2018), Canadians want privacy and security, but citizens often take risks online. They use free online services, including social media platforms, without realizing the cost of admission—their personal privacy.

CIRA's research shows that 80% of Canadians believe that universal access to high-speed internet is critical for economic growth in Canada and for prosperity.

CIRA also found that Canadians are quite unsettled about the spread of misinformation online, particularly in the face of the federal election later this year. And this is especially concerning given that 6 out of 10 Canadians surveyed had admitted they have been taken in by fake news. It is becoming more and more difficult to differentiate what's real and what's not, which is having a real impact beyond the digital world.

Encouraging Canadians to become digitally literate is one way to mitigate the risk. But it goes beyond just internet users.

Key Insights

- The impact of global discrepancies, internet administration, as well as specific activities conducted by states, has an effect at home. These affect the safety and security of Canadians online today, and the future of the internet.
- The reach of bad actors in various forms is cause for heightened concern, giving pause, and shifting perspectives. It is vital to ensure that a broader diversity of views are not lost along the way, including those of individual Canadian internet users.
- Increasing the digital literacy of Canadians will mitigate privacy and security risks, but other players also have a role in addressing these issues.

Opening Keynote Address: Elliot Noss, President & CEO Tucows

Key Issues

- Power of the internet to affect social and political change on a global scale.
- Potential strengths and limitations of the multistakeholder model and Canada's role within it.
- Impact to sovereign states of the multistakeholder model and local movements.
- Solutions must be global and cross-jurisdiction not national, in scope.

Elliot Noss
President and Chief Executive Officer of Tucows

Overview of Remarks

Problems of global magnitude cannot be solved by national remedies. Despite their revolutionary power as a force for change, nation states have failed to create a framework for internet regulation.

Canadians have a unique opportunity to contribute to global challenges through the multistakeholder model. While there are many multilateral, multinational problem-solving groups, ICANN is the only one wherein nation states sit as peers alongside other stakeholders.

The internet facilitates the transfer of power from nation states to the local level in a way never before seen. No longer restricted to geography, people can now connect with those with similar interests all over the world.

Nation states are unsuccessfully attempting to horizontally address problems that exist vertically. Trying to solve global issues through a national or international lense as opposed to a global approach will fail because the incentives are misaligned. This leaves addressing these problems open to anyone who can gather interest to commence multistakeholder processes for specific subject matters. A natural area where a multistakeholder process could evolve is with cybercrime.

Canada has a unique role and opportunity. We had a unique opportunity in the ICANN process where Canadians have been disproportionately involved. Canadians have made a tremendous impact to date and are well positioned to continue to do so in the future. Chiefly, Canada has two advantages: a) we are perceived as objective actors; and b) we have grown up as one of the only post-nationalist countries in the world.

There is no shortage of venues for all stakeholders to become involved in issues of internet governance and internet policy generally. ICANN is one of the few multistakeholder bodies to which nationstates have formally devolved responsibility. Furthermore, corporate efforts such as Sidewalk Labs are often surprisingly receptive to a wide range of stakeholders, including end-users. However, he cautioned users to realize the potential of these opportunities to be more constructive rather than alarmist/incendiary.

Key Insights

- Multi-stakeholder model is particularly well-suited for global challenges that transcend national borders and jurisdictions. Cybercrime and cybersecurity was a specific example.
- Trying to solve global issues through a national or international lense as opposed to a global approach will fail as incentives are misaligned.
- Canadian stakeholders have a unique opportunity to contribute to the challenges of the multistakeholder model.
- End-users and civil society organizations are constructive contributors in internet governance fora.

Megan Kruse
Business Director of the Internet Society's Online Trust Alliance

Considerations for Effective Internet of Things Labels

Panelists

- Megan Kruse, Internet Society's Online Trust Alliance (Moderator)
- Faud Khan, TwelveDot
- Sarah Ingle, Youth Internet Governance Forum Canada
- Elliott O'Brien , ecobee
- Maryse Guénette, Option consommateurs

Key Issues

- Consumer awareness.
- Mitigating cyber-threats.
- Vendor versus consumer responsibility.
- Standards and labels.

Discussion Overview

Consumers, mainly young people, are highly conscious of the collection and use of their data. There is a need for a coordinated approach to rebuilding trust in a legitimate and sustainable way with government, civil society, and the private sector.

The level of concern about privacy and security issues exceeds the level of awareness. In the very recent past, there was an expectation from consumers that their privacy and security were being considered before devices were put on the shelves. Now, in light of so many data breaches and data mismanagement scandals, there is widespread agreement that consumers and youth are generally more skeptical of manufacturers. However, this distrust has also sparked a keen interest in the way data is being collected, and the transparency manufacturers exhibit.

Standards and labels can be a practical option for consumer awareness and rebuilding trust. Examples were provided such as those working at the ISO level. The Standards Council of Canada has also been tasked with standards from the recent federal cybersecurity strategy. Many other standards have been or are being developed. This includes GDPR, the California Privacy Act and individual company IoT frameworks. Given Canada's limited market size, it is essential to look at what is happening globally with the European Framework and activities in the United States, and Japan. Canada needs international standardization or an international equivalency, at a minimum, to remove barriers to industry adoption.

There is a need to communicate with consumers using plain language. Moreover, consumers must be allowed to revoke consent at any time.

Many vendors are embracing the idea that security and privacy expertise is critical to their brand reputations. Labeling initiatives allow vendors to demonstrate through a trusted label, from a reputable third party, that they care about consumer privacy and security.

Key Insights

- Manufacturers are predisposed to approach labels as a legal requirement, as the case has been in the past. Going forward, however, label requirements cannot just be crafted by lawyers, and should be created with a user-first approach in mind.
- Global equivalency (both legally/jurisdiction, and in terms of relatability/language) is a requirement. International collaboration and standardization of an IoT security and/or privacy label is highly important.
- Consumer education – with a multi-stakeholder approach to determining and disseminating information – is essential to support a label and the underlying objectives. Consumer education and awareness campaigns in "Canadian" languages – French, English, and Indigenous – with pre and post-sale information – are needed.
- Increased transparency from manufacturers regarding security/privacy issues is critical.
- Whether voluntary or mandatory, a labeling framework will help build trust with vendors.

Misinformation, Bots, and Democracy

Panelists

- David Fewer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC) (Moderator)
- Kevin Chan, Facebook Canada
- Anatoliy Gruzd, Canada Research Chair in Social Media Data Stewardship
- David Skok, The Logic

David Fewer
Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC)

Key Issues

- Fake news and misinformation.
- Hateful online speech.
- Global and domestic threats.
- Data security.

Discussion Overview

The panel's discussion surrounded three main topics: 1) While foreign actors are a threat, domestic actors are an equal or higher risk when it comes to the dissemination of fake news and the proliferation of hateful speech online. Social media platforms also have to balance discouraging fake news, while ensuring they are not censoring a legitimate group; 2) Political actors are increasingly using social media platforms as a tool to get messages out; and 3) In the aftermath of Cambridge Analytica, academics have seen social media platforms reduce their access to datasets to study the fake news problem.

A recent report on Canadians' use of social media shows that 94% of internet users here in this country have at least one social media account. The exposure to potential misinformation and disinformation campaigns is enormous.

Both technological and policy-based solutions are needed to confront the fake news problem. Facebook, for instance, has a three-pronged strategy focusing on people, technology and, increasingly, partnerships. Facebook has gone from 10,000 to 30,000 people dedicated to working on this challenge. In Q2 and Q3 of last year, Facebook removed approximately 1.5 billion fake accounts.

The development of digital literacy skills is required to help users discern between real and fake news. The need for civility among users was also stressed.

Canada must decide on its approach to fake news and newer technology, generally. Do we want to follow the lead of the United States or Europe?

A void has been created in the news world because traditional journalism is fading quickly. Social media platforms have become a new distribution channel for news. Panelists disagreed on whether the problem can be solved through technology or if it is more deeply rooted in human causes for which technology has no response.

Key Insights

- There are local and foreign actors. At times international actors will see an advantage to fuelling a local misinformation campaign because it is aligned with their objectives and it is not always clear when they are working in conjunction with domestic actors.
- Individuals are often tricked into supporting a cause (e.g. supporting an event that is inauthentic).
- While AI can be used to detect bots and inauthentic accounts, a human reviewer is still a critical component. An understanding of the local culture and knowledge of its political dynamics are essential. There are technical limitations.
- While Facebook is often in the limelight, other platforms and websites are involved in misinformation.
- Attention must be given to whom platforms release data. Guidelines are needed to differentiate between releasing data to a private organization which may not have processes in place to ensure accountability over the safety and privacy of data, versus access to researchers who have institutional oversight, or research and ethics frameworks reviewing their work, and are trained to handle sensitive private data.
- It is critical to strike the right balance between not censoring legitimate content while ensuring we don't have bad actors and inauthentic behaviour on social media platforms.

Laura Tribe
Open Media (Moderator)

Privacy and Surveillance in the Internet Age

Panelists

- Laura Tribe, Open Media (Moderator)
- Vance Lockton, Office of the Privacy Commissioner of Canada
- Evan Light, York University
- Genevieve Lajeunesse, Crypto.Québec

Key Issues

- Government transparency.
- Lack of public awareness.
- GDPR/PIPEDA comparison.

Discussion Overview

There is not a full understanding on what government is doing around surveillance capabilities and how privacy is being affected. Without government transparency it is difficult to really understand how a conversation around privacy can begin.

Canadians are also often misinformed about privacy issues and, as a result, do not take into account matters such as transnational surveillance. Most people are not experts on the subject. For example, people may purchase services that might be vulnerable, and acquire services with the expectation that their privacy is protected. It was argued that the only way forward is to mandate approaches that are centred on privacy as a right.

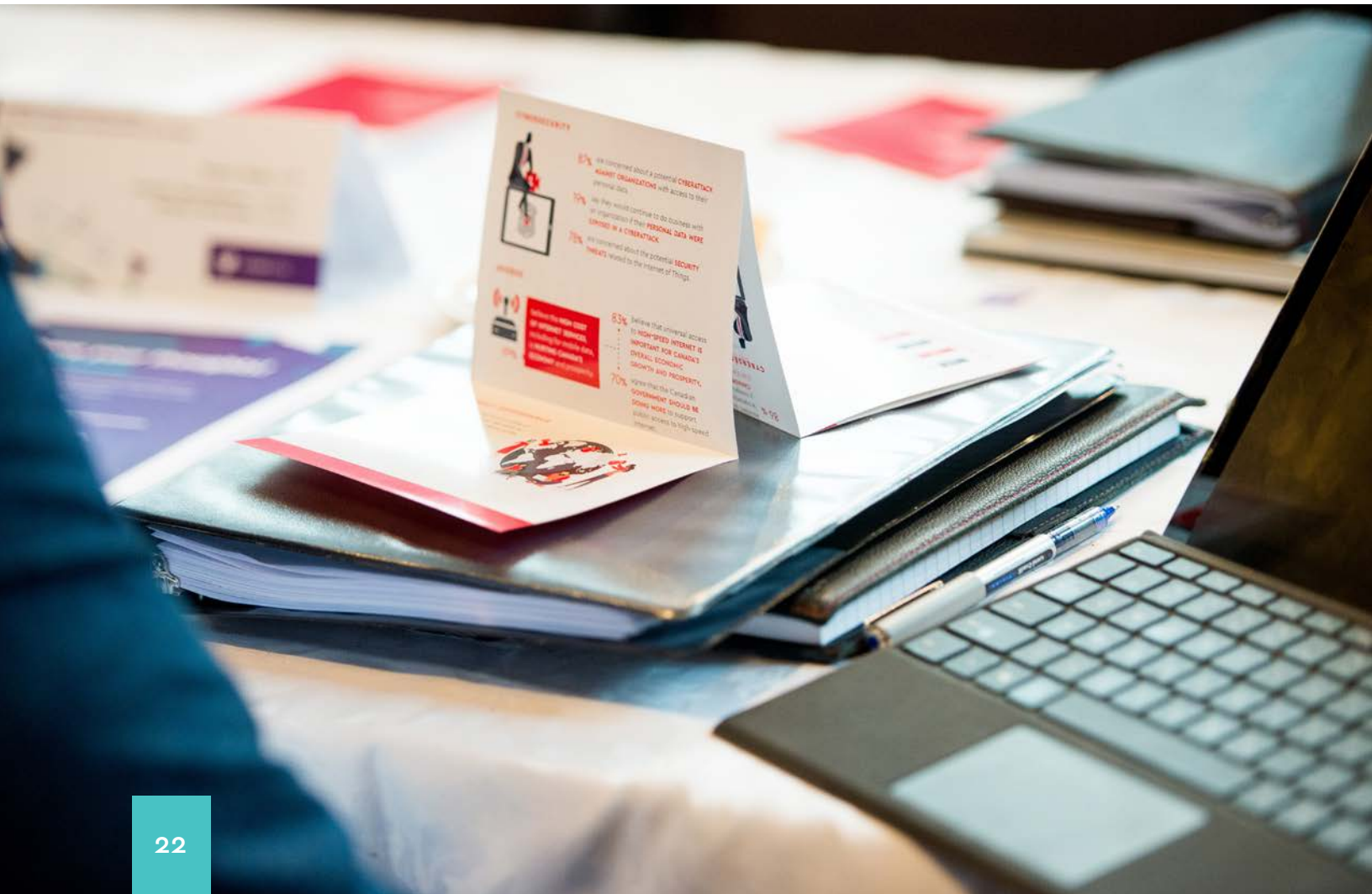
Barriers to establishing reasonable cause of a violation of privacy must be overcome. Before launching an investigation, exploratory work is necessary to identify if there is a problem, and if something needs to be done about it.

GDPR was discussed in comparison with PIPEDA, concluding that many of the guidelines are quite similar. The fundamental difference being the high financial penalties in Europe and whether these “scare tactics” are necessary to force compliance. On this note, it was brought up that importing GDPR into Canada may not be the answer, and that uniquely Canadian approaches may be necessary.

While corporate surveillance is a concern, it was raised that account breaches were often done by family members, for several reasons. Interestingly it was also brought up that many consumers feel uncomfortable using encrypted messaging because they feel as if they may be averting the law.

Key Insights

- Government transparency is necessary to fully understand what law enforcement and intelligence agencies are doing. The same should extend to corporate surveillance.
- Barriers to establishing reasonable cause of a violation of privacy must be overcome. Before launching an investigation, exploratory work is necessary to identify if there is a problem, and if something needs to be done about it.
- The consumer consent process must be concise and understandable.



Cybersecurity Challenges for Canadian Businesses

Panelists

- Dave Chiswell, Canadian Internet Registration Authority (Moderator)
- Bonnie Butlin, Security Partners' Forum
- David Shipley, Beauceron Security Inc.
- Scott Smith, Canadian Chamber of Commerce
- Tony Olsen, Canadian Centre for Cyber Security

Key Issues

- More education and resources required for SMEs to mitigate cybersecurity threats.
- Defining roles for government, business, and citizens. No single point of responsibility.
- Need for a transnational response to threats.

Discussion Overview

The repercussions of cyber threats are broad, and can have financial and reputational impact. This included consensus on the need for more education and resources.

There is a need to develop cybersecurity standard business practices, normalizing these activities in the same manner as other business practices. For example, locking up and depositing money in a safe or the bank.

Individuals have a responsibility to inform themselves but there is a need for a common and plain language approach for any general public or SME-focused practice to be successful.

There was also recognition that there are cohorts of consumers who may never completely understand the risks they are taking or how to protect themselves. This prompted debate on the role of government beyond education as well as what government's success rate has been. Some felt that law enforcement agencies, with responsibilities to protect citizens online, have completely failed to protect individuals from cybercrime. Others had empathy toward the challenges law enforcement agencies face, such as burden of proof. It was also noted that the Canadian Cyber Security Centre does have a role of working closely with stakeholders and government to develop policy more quickly to keep up with change.

Companies require crisis management plans so they can be as prepared as possible if they are impacted by a cybersecurity incident.

Key Insights

- There is a need for more and better resources to support and educate SMEs on cybersecurity.
- Ensure government policies and legislation keep up with pace of change.
- SMEs need to build processes to prepare against cybersecurity threats, and crisis management plans in case an incident occurs. SMEs must consider cybersecurity in the same terms as physical security.
- Cybersecurity insurance is one tool in the cybersecurity toolbox, but it is complex and has numerous limitations.

Are we Building a More Equitable and Inclusive Future?

Panelists

- Sarah Ingle, Youth IGF Canada (Moderator)
- Joe Catapano, ICANN
- Nasma Ahmed, Digital Justice Lab
- Raman Dang, Microsoft Canada
- Honey Dacanay, Government of Ontario
- Kate Kalcevich, Government of Ontario

Key Issues

- Need for inclusion.
- Role for young people.

Sarah Ingle
Youth IGF Canada

Discussion Overview

Inclusion needs to be embedded from the beginning, not pursued as an afterthought. A haphazard approach will not result in true inclusion and diversity. Diversity can be achieved through hiring targets, the provision of resources, and mentoring to underrepresented groups.

Young people need to be at the forefront of conversations about internet governance, digital rights, public-private partnerships, and policy-making processes. It is necessary to better support their participation.

A lot of important work in this area is on a voluntary basis, unpaid, or precarious. This puts young people and historically underrepresented groups in a disadvantaged position to participate.

Key Insights

- Inclusivity needs to be embedded at the beginning rather than as an afterthought.
- Digital rights, literacy, citizenship, skills, etc. need to have more emphasis within curricula.
- Supporting public institutions and libraries as providers of important resources (e.g. tech support, internet hotspots, equipment rentals, workshops, etc).
- Better engaging the public, and other stakeholders, through consultation processes in order to facilitate participatory policy and service design.
- Recognizing the role of democracy and public institutions to sometimes move more slowly, carefully, and thoughtfully due to their wider responsibilities. Not to be rushed by private entities, and instead to balance preparedness with efficiency.

Canada's Role in the Future of Internet Governance

Panelists

- Fen Hampson, Centre for International Governance Innovation (Moderator)
- Farzaneh Badiei, Georgia Institute of Technology
- Paul Charlton, Senior Policy Advisor, Government of Canada
- Paul Andersen, EGATE Networks
- Konstantinos Komaitis, Internet Society

Fen Hampson
Centre for International Governance Innovation

Key Issues

- Canada's multi-stakeholder approach.
- Divide between security and internet governance.
- Jurisdictional fragmentation.

Discussion Overview

The Government of Canada is strongly committed to the multi-stakeholder approach. Collaboration has always been key to making the internet work and it is important to preserve this. Government is only one seat at the table among transnational elements of civil society, industry, etc. The future of internet governance will involve applying this approach to problems as they arise.

There is a tension between internet governance and security. On one hand governments are committed to the multistakeholder model. On the other hand they all have their security centres and frame the internet as a national security issue which does not lend itself to multi-stakeholder governance.

On jurisdictional fragmentation, benevolent and malevolent nation states are trying to create virtual borders on the internet. Generally, there are four "internet models":

- Silicon Valley (open, self-regulated).
- Washington D.C. (commercially-driven).
- European (becoming heavily regulated).
- China (authoritarian, very closed, surveilled).

European regulation has caused a rush for governance around the world and conflicting decisions. This has caused unintended consequences that trickle down to infrastructure. The most obvious is fragmentation, for instance a Supreme Court of Canada decision to delist some information from Google's global index. By contrast, the European Court of Justice said Google is not required to do this.

Despite shifting earth under our feet, much stays the same. Countries like Russia and China still want what they have always wanted: government-led internet with controlled content. Meanwhile, much of the West continues to resist this, instead advocating for an open internet and more light-handed regulation.

Canada has long punched above its weight in internet governance. For example, CIRA led on WHOIS privacy before GDPR was even a thought. There is an opportunity for Canada to continue to be a model of, and champion for, the multistakeholder approach.

Key Insights

- Regulation must respect the different layers of the internet and avoid unintended and/or cross-jurisdictional consequences.
- Stakeholders (particularly the technical community) must reach out to their governments to explain any unintended technical consequences of its regulation.
- Canada has the opportunity to learn from the regulatory and legislative experiences of the EU and USA, but it must adapt these lessons to the Canadian context.

Statement of Priorities

These conclusions reflect Canadian values of inclusion, global cooperation, and need to balance freedom online with accommodating others' rights. The keynote's discussion of Canada as a 'post-national' state was an intriguing concept that resonated with many stakeholders. It was acknowledged that Canada will contend with specific challenges (e.g., multilingualism, smaller market) but also has many advantages (e.g., being able to take the best of both the european and american approaches). Canada's broad and meaningful contribution to multistakeholder organizations and approaches (e.g., ICANN) builds off of our historic role on international consensus-building. The Canadian role is often understated, but well-regarded globally.

Priority 1: Maintain, develop, and promote the current multistakeholder approach to internet governance, both within Canada and internationally.

Internet governance issues cross borders and affect individuals, businesses, governments, and civil society. Because these issues are inherently global and multi-sectoral, national governments alone cannot adequately address them. Solutions pursued in a vacuum are likely to suffer from the misaligned incentives that come with using national or international approaches to address global problems. To encourage effective problem solving in internet governance, it is vital that we safeguard and build on the multistakeholder approach.

This priority reflects the Canadian value of cooperation. Historically, Canada's role on the global stage has been one of building consensus, brokering compromises, and promoting norms. Canada's broad and meaningful contributions to multistakeholder efforts, including ICANN, are a continuation of this legacy.

Priority 2: Encourage both governments and businesses to increase transparency of their operations to promote public trust and user empowerment.

Increasing transparency is a means to improve citizens' trust in their government and users' trust in internet-related products and services. Public trust is a major element of social capital, which can affect levels of political involvement and economic prosperity. Increased transparency about government and corporate surveillance also allows users to make informed decisions about their online behaviour. Using the multistakeholder approach is one way to improve transparency, as it tends to hold powerful actors accountable to civil society.

Canada has traditionally been a high-trust society. However, if left unchecked, internet-related issues such as privacy, surveillance, and misinformation could contribute to the erosion of this trust. Therefore, encouraging public trust through increased transparency and multistakeholderism should be a particularly high priority in Canada.

Priority 3: Ensure that internet governance solutions developed by all stakeholder groups are thoughtful, evidence-based, and proportionate.

Despite the urgency and high profile of internet policy issues, stakeholders must recognize the tradeoffs and complexities therein. For instance, efforts at combating online misinformation may censor legitimate users. While inclusive democratic processes are incredibly valuable, the development of policy must also keep pace with a rapid rate of change. The neglect of such nuances could result in "one size fits all" solutions, which are likely to be ineffective and may have unintended consequences.

Canadians have long been known for caution and careful reflection. These attributes can be taken to extremes; however, they can also help us to navigate complex issues. When a poorly thought-out policy can negatively affect multiple stakeholders in Canada and beyond, taking the time to consult the evidence is extremely valuable.

Priority 4: Raise awareness of internet governance issues among all stakeholders. In particular, educate users about how they can participate.

Stakeholders should consider the importance of education, outreach, inclusivity, and user-friendliness when developing solutions. It is not enough that individuals and organizations have the tools required to protect themselves online. They need to know how and why they should use them. This is particularly true when it comes to issues like privacy, cybersecurity, online misinformation, and the labelling of IoT devices. There are human elements in all of these issues that must be considered.

The keynote characterized Canada as a 'post-national' state, an intriguing concept that resonated with many stakeholders. Post-nationalism, along with Canada's ethnic and linguistic diversity, has entrenched inclusiveness as a Canadian value. Upholding the value of inclusiveness can ensure that outreach and education programs accommodate all Canadians

Future of the Canadian IGF

As a National-Regional Initiative (NRI) of the global Internet Governance Forum, this outcome document will feed into the agenda setting and discussion of the NRI community at the 2019 IGF in Berlin, Germany on November 25-29.

Going forward, the multistakeholder steering committee of the CIGF sees an opportunity to build a community of interest and a forum for ongoing discussion around the Canadian IGF. An open mailing list and newsletter have been created and are available at CanadianIGF.ca. Additionally, the CIGF is active on Twitter and Facebook.

The steering committee will utilize these channels to launch a public call for input on the substance of future meeting programs. This will ensure agendas encompass the views and concerns of the wider community.

The core steering committee is also seeking new members for the 2020 planning process in order to better reflect geographic and stakeholder diversity. In an early debrief, the steering committee agreed that the 2020 event would be held in a province other than Ontario, and is will seek out partner organizations interested in contributing to future Canadian IGF events in new regions of the country.