cira

BUILDING A BETTER
ONLINE CANADA

CANADIANS DESERVE
A BETTER INTERNET

06-02-2019

TABLE OF CONTENTS

FOREWORD

BY BYRON HOLLAND, PRESIDENT AND CEO

The internet has revolutionized the day-to-day lives of Canadians in how we communicate, work, shop and access services. This global resource connects us all, but it is not administered in a homogenous way around the world. Diverging ideologies have created an internet with stark differences from region to region, and contrasting philosophies within those regions.

There are the democracies of the West with an open, industry-driven internet versus more authoritarian states, with a command-and-control approach. Within each are variations. Some autocracies have more or less control, all the way up to the extremes of China and its Great Firewall. In the West, there is a contrast between the privacy regulations of Europe and the data-driven Californian internet, which is largely the internet Canadians experience.

The impacts of these global discrepancies, as well as activity taking place closer to home, affect the safety and security of Canadians online today, and the future of the internet as we know it.

In the age of fake news and election interference, Canadians are unsettled by the viral spread of misinformation on their social media channels. Most of the free online services Canadians have come to enjoy have a cost – our personal information. Demographic and psychographic profiles of our online activities are immensely valuable. Canadians' personal data powers the ad networks to nudge users toward specific purchases and algorithms driven by users' online activity serve up targeted online content.

While this digital advertising machine may mean more convenience for some Canadians, and in spite of users' affinity for these free platforms and online services, Canadians are concerned about how companies collect and use their personal information[1]. After all, it's rare that a week goes by without a cyberattack or security vulnerability making headlines.

[1] Findings from CIRA's research, December 2018/January 2019, refer to the privacy section of this report.

Even with all of that, the internet in Canada is a powerful force for good—enabling access to knowledge, underpinning commerce and connecting us to communities of interest at home and abroad. The majority of Canadians now have internet access. Notwithstanding inequities in the quality of that access, the internet is, for the most part, ubiquitous in the lives of average Canadians.

Yet, the open internet envisioned by the early luminaries of networking and the World Wide Web is being challenged on a number of fronts: misinformation, privacy, security, access and governance.

The internet was designed to be open and interoperable. The architecture allows anyone with a modem to connect her or his host to the network. This utopian vision for collaboration and community has resulted in an architecture that is inherently vulnerable to malicious players seeking to ruin everyone else's fun. The openness of the internet is both its strength and its weakness.

While internet governance has primarily focused on protocols of the internet, today's governance must carefully account for increasing malicious activity on the internet. At the content level, there is a proliferation of fake news, hate speech and invasions of personal privacy. At the infrastructure and protocol levels, large-scale attacks have become commonplace.

The only way to meaningfully address these complex, supranational issues is through engagement between governments, civil society and the private sector about internet governance. This is new territory for everyone involved, but it's also an opportunity for citizens to demand the internet they want and deserve from industry and policy-makers.

As the steward of the .CA domain on behalf of all Canadians, and as an active participant of internet governance, CIRA seeks greater understanding of the issues, and solutions for a better online Canada. In December 2018, CIRA surveyed Canadians to learn more about their opinions and experiences online. The following report breaks down these experiences and what Canadians want

for Canada's internet. Unfortunately, the concerns are many. However, so too are possible solutions. Based on CIRA's research, Canadians see three key players: government, business and citizens themselves.

As internet advocates, stewards, policy-makers and experts gather for the 2019 Canadian Internet Governance Forum, we must listen to Canadians and work together to meet their demands. They deserve our full attention and action on a resource so central to most Canadians' everyday lives. Ultimately, Canadians deserve a better internet – and it's up to all of us to provide it.

KEY FINDINGS IN THIS REPORT

Of Canadian internet users:

SOCIAL MEDIA AND FAKE NEWS

- **75%** say they come across fake news at least sometimes.
- **57%** have been taken in by a fake news item.
- **70%** are concerned that fake news could impact the outcome of the next federal election.

PRIVACY

- **72%** are willing to disclose some or a little personal information in exchange for a valuable/convenient service.
- **87%** are concerned that businesses with access to customers' personal data willingly share it with third parties without consent.
- **86%** believe it is important that government data, including the personal information of Canadians, be stored and transmitted in Canada only.

CYBERSECURITY

- **87%** are concerned about a potential cyberattack against organizations with access to their personal data.
- Only **19%** say they would continue to do business with an organization if their personal data were exposed in a cyberattack.
- **78%** are concerned about the potential security threats related to the Internet of Things.

ACCESS

- **69%** believe the high cost of internet services, including for mobile data, is hurting Canada's economy and prosperity.
- **83%** believe that universal access to high-speed internet is important for Canada's overall economic growth and prosperity.
- **70%** agree that the Canadian government should be doing more to support public access to high-speed internet.

INTERNET GOVERNANCE

- **75%** say they only know a little or hardly anything about the topic of global control and regulation of the internet.
- **50%** are concerned that the global internet could fracture into regional blocks that adopt very different regulatory principles and policies.
- **66%** support the principles of net neutrality.

I. TRUST IN CONTENT: COUNTERING FAKE NEWS ONLINE

In the early days of the internet, when everyday citizens began accessing websites and email, online content was new, exciting and interesting. But, what online content wasn't, was trusted.

Anyone who went to university in the late 1990s or early 2000s will remember that universities rarely accepted online sources as these had not gone through the fact-checking of a peer review. Students of the time relied on tried and true methods of research, primarily found in a library. The online world was new and most people were not yet comfortable with its content.

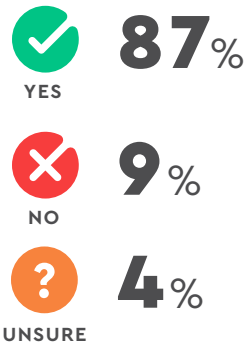
Fast forward 20 years, and online content permeates the schools, workplaces and living rooms of nearly all Canadians. Readership of trusted sources of the past including newspapers, which have their own journalistic standards, are on the decline as eyeballs turn to the internet. In fact, academic research papers, respected newspapers and magazines, and many other sources of news and information are now accessed easily online alongside content without the same stringent editorial review processes.

According to Canada's Internet Factbook 2018[2], 55 per cent of Canadian internet users access news and current events via the internet. Whether via subscription or otherwise, Canadians now get their news online.

When thinking about the pervasiveness of online content and news – in sharing it and accessing it – one cannot ignore the rising concern among Canadians about fake news, or fabricated news stories that grossly misrepresent actual events. On this front, three quarters of Canadian internet users say they at least sometimes encounter fake news online, and the majority agree that it's a problem.

[2] Canada's Internet Factbook, 2018, internetfactbook.ca

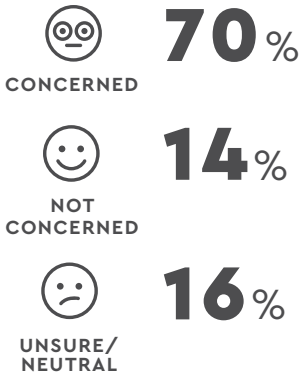
Percentage of respondents that agree the spread of fake news on social media is a problem



Questions around the influence of fake news on the 2016 U.S. presidential election highlight the growing need to analyze the power and prevalence of fake news. Fake news takes many forms, and can include wholly inaccurate content, news that misrepresents facts or is biased, and old stories passing as current news. It can also include echo chambers, whereby social media sites serve users imbalanced content, largely through algorithms based on their past online behavior, confirming and supporting views the user already holds or leans toward.

The lessons learned south of the border have encouraged 70 per cent of Canadian's surveyed to express concern that fake news could impact the outcome of the next Canadian federal election. The urgency in this case is clear.

Level of concern that fake news could impact the next Canadian federal election



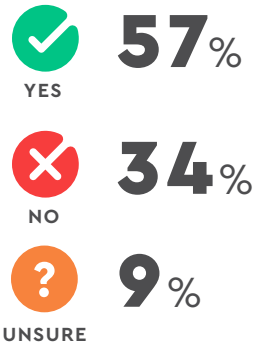
SOCIAL MEDIA AND SPREADING MISINFORMATION ONLINE

Where does fake news flourish and how is it spread? To many, the answer lies in social media platforms.

CIRA's research indicates that 80 per cent of social media users read or listen to news items shared by others and about a third share news items with others via social media. Given that nearly 70 per cent of internet users in Canada say they access a social media site almost every day, this is worth reflection.

Consider as well that while eight in ten Canadians are confident in their ability to recognize fake news stories online, just one quarter are very confident. Of greater concern, over half of Canadians admit they've been taken in by a fake news item.

Percentage of respondents who believed what they later found out to be fake news



STOPPING THE SPREAD OF FAKE NEWS: THE ROLE OF GOVERNMENT, SOCIAL MEDIA COMPANIES AND THE MEDIA

If you ask Canadian internet users, they see the responsibility to stop the spread of fake news split between social media companies, the press, the federal government and citizens themselves.

Responsibility to stop the spread of fake news

72% SOCIAL MEDIA COMPANIES

68% MEDIA/PRESS/BROADCASTERS

67% CITIZENS THEMSELVES

63% JOURNALISTS

50% FEDERAL GOVERNMENT

8% OTHER/DON'T KNOW

When asked which of these should have the responsibility in monitoring and removing fake news from their platform, 91 per cent say social media should have at least some responsibility and nearly half of Canadians say these companies should have complete responsibility.

Social media companies, including Facebook, have begun to react. In April, 2018, Facebook published a blog[3] outlining the "70 Facebook and 65 Instagram accounts – as well as 138 Facebook Pages – that were controlled by the Russia-based Internet Research Agency," that were removed to counteract the spread of fake news on their platform.

At the DLD conference in January 2019, Facebook COO Sheryl Sandberg shared five things Facebook would do in 2019[4] to counter fake news. Two questions remain though. Is this action enough? Moreover, is it too little too late?

[3] Authenticity Matters: The IRA Has No Place on Facebook https://newsroom.fb.com/news/2018/04/authenticity-matters/

[4] Stung by criticism, Facebook's Sandberg outlines new plans to tackle misinformation, https://techcrunch.com/2019/01/20/stung-by-criticism-facebooks-sandberg-outlines-new-plans-to-tackle-misinformation/

A majority (79 per cent) of Canadians want the federal government to impose fines or other sanctions on social media companies that do not act to remove fake news from their platforms. To date, the Canadian government has not taken such drastic action. In advance of the upcoming federal election, the Government of Canada has announced a five-member panel of senior bureaucrats that will analyze threats and inform political parties and the public of those threats.[5]

With or without government intervention, social media companies have a responsibility to stop the spread of fake news. However, given the speed with which news travels online, social media companies cannot stop fake news alone. In addition to the government and social media companies, Canadians also see traditional media and journalists as catalysts to stop misinformation from spreading online.

While most Canadians are at least somewhat confident that the information they access through major newspapers, TV news networks and radio stations in Canada is generally fair and accurate, few say the same of video hosting websites, podcasts and social media/messaging apps.

Confidence that news/ information is generally fair and accurate

81%
MAJOR NEWSPAPERS (PRINTED/ONLINE)

80%
TV NEWS NETWORKS

78%
RADIO STATIONS

27%
VIDEO HOSTING WEBSITES AND PODCASTS

21%
ONLINE SOCIAL MEDIA SITES AND MESSAGING APPS

[5] Federal plan to protect elections does not include controls on social-media platforms, Globe & Mail, January 30, 2019, https://www.theglobeandmail.com/politics/article-federal-plan-to-protect-elections-does-not-include-controls-on-social/

Given that trust exists in more traditional media sources, Canadian journalists can help thwart fake news online. Whether through fact-checking or countering false information spreading online, journalists are in a position to make a positive impact. However, with a shrinking traditional media landscape whereby roughly one-third of journalism jobs have been lost in the past six years[6], how long can Canadians rely on this valuable source of information?

INDIVIDUAL CANADIANS CAN STOP THE INFLUENCE OF FAKE NEWS

What are the responsibilities of citizens themselves? Canadians are alert to the possibility of fake news online, but how can they be sure when they encounter it?

Digital and media literacy are important for all Canadians to better navigate the online world – and Canadian internet users agree.

agree that Canada's public schools should place more of a focus on **digital literacy** for students.

agree that Canada's public schools should place more of a focus on **media literacy** for students.

Canada is investing in digital literacy. For example, the federal CanCode program invested over $50 million to support initiatives providing educational opportunities for coding and digital skills for Canadian youth from kindergarten to grade 12[7].

[6] Canadian news industry at crisis point, suggests new report, CBC, https://www.cbc.ca/radio/thecurrent/the-current-for-january-27-2017-1.3953609/canadian-news-industry-at-crisis-point-suggests-new-report-1.3953678 with full report: https://shatteredmirror.ca/wp-content/uploads/theShatteredMirror.pdf

[7] CanCode, from Innovation, Science and Economic Development Canada, https://www.ic.gc.ca/eic/site/121.nsf/eng/home

As well, the Canadian government announced $7 million in funding this past January to fight the spread of fake news online. The funding will be split between organizations conducting digital literacy programs to help voters better assess online information and groups working to increase understanding of disinformation[8].

Both Facebook and Google are also funding similar support initiatives, with Google giving $500,000 to the Canadian Journalism Foundation and Civix to teach students to recognize fake news online[9]. Facebook has also launched a "digital news literacy campaign" with the digital and media literacy organization MediaSmarts[10].

Organizations like CIRA are investing in this important value-add as well. Like Facebook, CIRA supports MediaSmarts. CIRA recently provided over $80,000 to MediaSmarts to carry out qualitative research for Phase IV of Young Canadians in the Wired World[11], which tracks and investigates the behaviours, attitudes and opinions of Canadian children and youth with respect to their use of the internet. This research will provide the foundation and direction for the quantitative classroom-based research instruments for a national survey to follow. Considering how many Canadian adults have been taken in by fake news, arming children with media literacy skills early on is important.

With only a quarter of Canadians fully confident they can recognize fake news online, these investments – both time and money – are much needed.

[8] Federal government to announce $7 million in funding to fight disinformation online ahead of 2019 election, The Logic, January 29, 2018, https://thelogic.co/news/exclusive/federal-government-to-announce-7-million-in-funding-to-fight-disinformation-online-ahead-of-2019-election/?gift=90e7f4480bfff7a20e89a0ca384cc3d9

[9] Google bankrolls Canadian school program targeting fake news, The Star, September 19, 2017, https://www.thestar.com/news/gta/2017/09/19/google-bankrolls-canadian-school-program-targeting-fake-news.html

[10] Facebook launches 'election integrity initiative' to fight hacking and fake news, CBC, October 19, 2017, https://www.cbc.ca/news/politics/facebook-election-hacking-fake-news-1.4362002

[11] Young Canadians in a Wired World, Phase III: Life Online, MediaSmarts, http://mediasmarts.ca/ycww/life-online

II. PRIVACY

Canadians value their privacy. In fact, six in ten Canadian internet users say they value it over convenience with only seven per cent saying convenience was more important to them than privacy.

Which is more important – convenience or privacy?

7%
CONVENIENCE

63%
PRIVACY

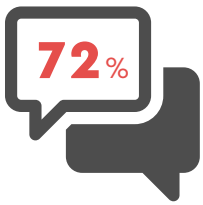
23%
DEPENDS ON THE SITUATION

6%
IT'S TOO HARD TO CHOOSE

1%
UNSURE

However, while Canadians value it and say they want it, they make choices online that put their privacy at risk.

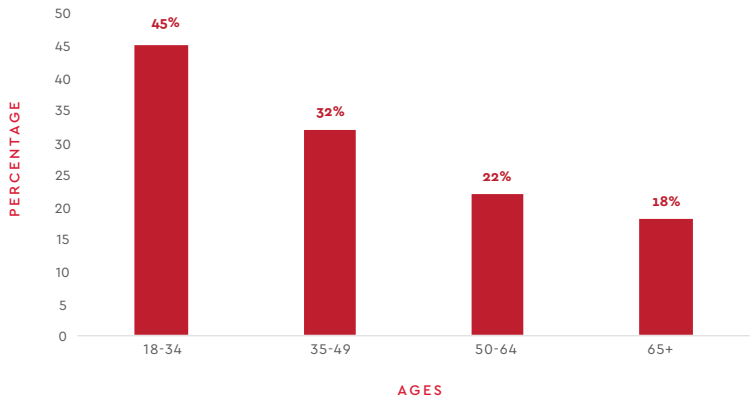
For example, many Canadians visit a social media site every day. These sites, along with many websites, are free to use, where the cost of admission is the user's information. This feeds advertisers the data to target users and serve them ads. In fact, many Canadians say they are willing to disclose some personal information in exchange for a valuable or convenient service.



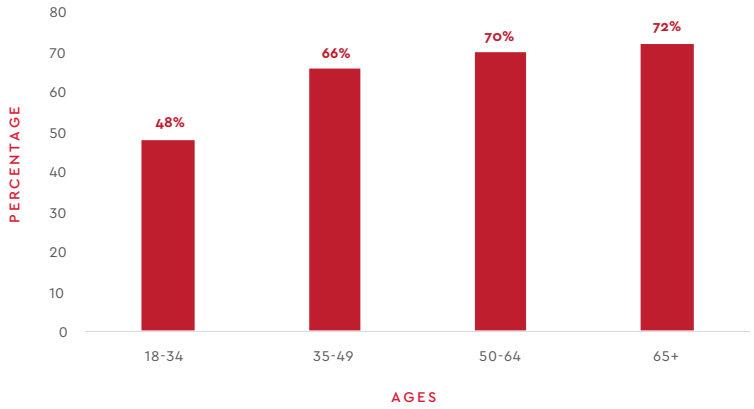
Are **willing to disclose 'some' or 'a little'** private/personal information for a valuable or convenient service

This willingness decreases with age whereby 18–49 year olds are more willing to give up a 'great deal' or 'some' private information versus those over 50.

Willingness to give up a great deal/some private or personal information for a valuable or convenient service



People who indicate they value privacy over convenience

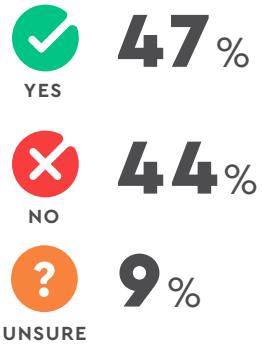


At the same time, nine in ten Canadians are concerned that businesses with access to personal data willingly share it with third parties without consent and over half of Canadian internet users say they are willing to share personal information in exchange for better programs and services from the government. On this note as well, nearly half (42 per cent) support sharing Canadians' personal information with law enforcement agencies, with some restrictions. Though, seven per cent support this with no restrictions.

CANADIAN DATA TRAVELING SOUTH OF THE BORDER

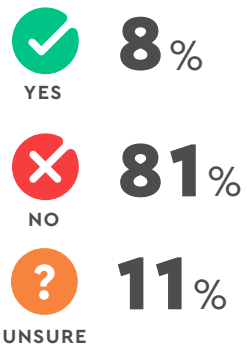
While most Canadian internet users (78 per cent) are concerned about the security and privacy of their personal information if stored in or routed through the United States, only half of Canadians are aware that many cloud services in Canada store data on servers located in the U.S. Even fewer are aware that some communications intended to begin and end in Canada run through the U.S.

Awareness that some of Canada's internet infrastructure runs through the U.S.



Even worse, 79 per cent of Canadian internet users say, if given a choice, they would prefer to use cloud services whose servers are located in Canada (and thus regulated under Canadian privacy laws). However, a mere eight per cent of cloud service users have ever switched to one based in Canada. Canadians appear to understand the risk, but fail to act against it.

Incidence of switching cloud services to use one whose servers are located in Canada



Canadians want to have their cake, and eat it too. They want more privacy, but they also want greater convenience. They want businesses, their government and law enforcement to access private information in order to provide better services, but they remain concerned with what happens to their personal information. How can Canadians have the convenience they desire, while remaining secure in the knowledge that their privacy is protected online?

ENHANCING PRIVACY PROTECTION

One solution could be tapping into the willingness of some Canadians to pay more for online services. Currently, the currency online is personal data. Data has recently been dubbed the new oil, indicating the value of this resource.[12] Given that six in ten Canadians say they would pay more for products and services that guarantee protection of privacy and personal data, this could be an option for some Canadian businesses. However, it remains to be seen whether Canadians' willingness would remain strong if presented with an actual dollar amount.

Canadian businesses are taking action in other ways too. According to CIRA's cybersecurity survey[13], released in October 2018, the top reason Canadian businesses devote resources to cybersecurity measures is to protect the information of their customers.

[12] The world's most valuable resource is no longer oil, but data, The Economist, May 2017, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

[13] Fall 2018, Cybersecurity survey, CIRA, https://cira.ca/2018-cybersecurity-survey-report

Despite this, more can and should be done. Canada has regulations in place around privacy. The Personal Information Protection and Electronic Documents Act (PIPEDA) is the Canadian federal privacy law for private-sector organizations. While 59 per cent of small-to-medium sized businesses that responded to the fall CIRA cybersecurity survey said they stored personal information from customers, only 38 per cent said they were familiar with PIPEDA[14].

In November, significant changes were made to PIPEDA, impacting Canadian businesses of all sizes, including new mandatory breach reporting requirements. There are penalties, with fines up to $100,000 for non-compliance.

Businesses need to understand the laws in place and must follow them.

Another approach might be enhanced Privacy by Design methodology, developed by Ann Cavoukian, the former Information and Privacy Commissioner for Ontario. This framework considers

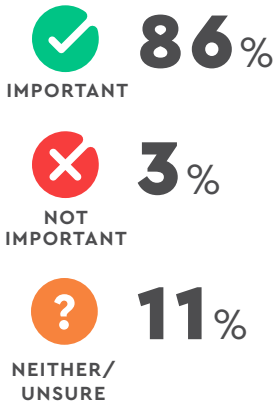
[14] Fall 2018, Cybersecurity survey, CIRA, https://cira.ca/2018-cybersecurity-survey-report

privacy throughout the engineering process. However, this approach is imperfect and has been "criticized as being vague, difficult to enforce its adoption, difficult to apply to certain disciplines, as well as prioritizing corporate interests over consumers' interests and placing insufficient emphasis on minimizing data collection". [15] That said, the European General Data Protection Regulation (GDPR) incorporates Privacy by Design. Could there be aspects of this framework worth considering further in a Canadian context?

CANADIAN INFRASTRUCTURE CAN ENHANCE PRIVACY PROTECTION

Eight in ten Canadian internet users believe that government data, including the personal information of Canadians should be stored or transmitted in Canada only. Of those Canadians, over half believe this is critically important.

Importance that government data be stored/transmitted in Canada only



[15] Privacy by design, Wikipedia, https://en.wikipedia.org/wiki/Privacy_by_design

Given that some Canadian data travels across the Canada-U.S. border, even data intended to stay local, what is the Canadian government doing to ensure the private data of Canadians is protected?

The Canadian government has an opportunity available to them right now to support greater privacy protection of its citizens. Infrastructure investments, including investment into Canadian internet exchange points (IXPs), increase the chance that data intended to stay within Canada's borders can do so.

An IXP is a hub where those who peer at it can exchange data directly. This avoids the need to take the long route, which often results in exchanges occurring in the U.S. Once that data crosses the border, Canadian privacy laws no longer apply. Given the Edward Snowden revelations of NSA surveillance programs in the U.S., this should be of concern for all Canadians.

With 11 IXPs up and running, Canada is doing well. However, these exchange points require a critical mass of participation and currently, most large enterprises, governments and large internet service providers are not using them. We need Canadian online entities to understand the value of Canadian IXPs and grow the number of organizations peering at them. One of the biggest impediments is the lack of peering by Canada's largest internet service providers.

Through greater participation and investment in Canadian IXPs, and other infrastructure such as cloud services and other hosting facilities that could be built in Canada, Canadian data meant to stay local, can do so.

III. CYBERSECURITY

Cybersecurity threats are a part of the online world. With reliance on digital technology growing, these threats are growing as well. Nearly 90 per cent of Canadian internet users are concerned about cyberattacks against organizations that access their personal data. Only two in ten say they would continue to do business with an organization if their personal data were exposed in a cyberattack, though our research does not show how many Canadians have actually actioned that sentiment.

Respondents concerned about cyberattacks

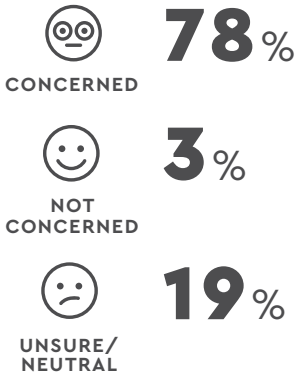
This is a valid concern given that 40 per cent of businesses who responded to CIRA's fall cybersecurity survey in 2018 admitted they had experienced a cyberattack in the last 12 months. Among larger businesses (250–499 employees) this number increases to 66 per cent. Overall, one in ten experienced more than 20 attacks[16]. Cybersecurity is a major issue and one that must be addressed from all sides.

[16] Fall 2018, Cybersecurity survey, CIRA, https://cira.ca/2018-cybersecurity-survey-report

THE INTERNET OF THINGS

Nearly half of Canadians have at least one smart-home device. That includes items such as intelligent light bulbs, smart thermostats or security devices such as Wi-Fi enabled cameras or internet-connected door locks. Eight in ten Canadian internet users are concerned about potential security threats related to IoT devices.

Concern about potential security threats related to IoT devices



While Canadians' concerns around IoT might be focused on personal security, where hackers can get into video camera feeds or take control of a door lock, CIRA's Chief Technology Officer Jacques Latour sees the risks on a much larger scale. "Day-to-day use is not the biggest concern. It's when there is a zero-day event that impacts a lot of devices all at once that I worry about."

Latour explains, "There is the good and bad of IoT devices. Some devices are well designed and secure. Those are not of concern. But, there are devices out there that we need to watch out for. Many of these cheaper devices are less secure and use similar software applications as each other. That means that if those applications become compromised, that can turn into a large-scale attack affecting hundreds or thousands of devices."

It's at that point where IoT devices can be used to launch an attack on an online service or part of the larger internet. These types of attacks, called distributed denial-of-service attacks (DDoS), can take down the internet, as the Mirai attack on Dyn did in 2016, affecting many websites and online services including Netflix, Amazon, CNN, Shopify and VISA[17].

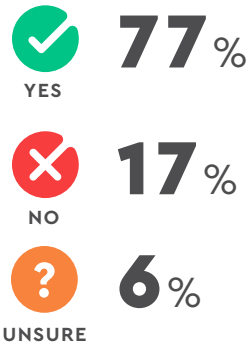
Latour represents CIRA in a multistakeholder process to identify and guide the development of IoT policy in Canada, which includes the Government of Canada, the Internet Society, CIPPIC and CANARIE. Latour is also working on a CIRA secure home gateway that can help secure smart-home, IoT devices on a user-friendly platform to keep Canadians safe from attacks coming from the internet, and the internet safe from compromised IoT devices.

As the organization that manages the .CA domain on behalf of all Canadians, ensuring CIRA's servers and the .CA domain registry is secure, is a top priority. Insecure IoT devices pose a clear risk to CIRA, the entire .CA space, as well as others who operate an internet business.

INVESTING IN CYBERSECURITY

Most Canadian internet users (82 per cent) believe the government should regulate how data collected through smart-home devices is used and protected. Additionally, 77 per cent believe the government should provide resources and infrastructure to Canadian businesses to help protect them from cyberattacks.

Should the government provide resources/infrastructure to protect businesses against cyberattacks?



[17] 2016 Dyn cyberattack, Wikipedia, https://en.wikipedia.org/wiki/2016_Dyn_cyberattack

The government could be investing more and Canadian businesses must prioritize cybersecurity.

Nearly a third of businesses who responded to CIRA's cybersecurity survey in the fall 2018 said they would add cybersecurity staff in the next year, which is good news. However, given that 37 per cent of those survey respondents did not have anti-malware protection installed and a shocking 71 per cent did not have a formal patching policy – additional investments in cybersecurity are much needed[18].

But it doesn't stop with malware protection and cybersecurity services. Human beings are one of the biggest cybersecurity threats businesses face. Phishing attacks directly exploit employees' points of weakness and according to CIRA's fall cybersecurity survey, only half of businesses provide cybersecurity training for their employees.

CIRA developed the D-Zone DNS Firewall to protect Canadian organizations from ransomware, malware and phishing attacks. For organizations without malware protection, a DNS filtering mechanism like the one CIRA has can help avoid connecting to malicious sites.

"It's a level of protection that should be sponsored by the government," says Latour. "Think of it like water. You don't ever think about clean drinking water until you get sick, and the government has regulations and support in place to make sure that doesn't happen. Malware protection at the DNS-level helps an organization stay 'healthy' on the internet in much the same way."

Cybersecurity is not an all-or-nothing proposition. There is no way to be perfectly cyber secure. However, organizations can and should do all they can to stay one step ahead of would-be attackers. This takes a multi-layer approach and there are responsibilities across the board. Government, business and individual alike.

[18] Fall 2018, Cybersecurity survey, CIRA, https://cira.ca/2018-cybersecurity-survey-report

IV. ACCESS

In June, 2018, Tracey Axelsson, executive director of the non-profit internet service provider Vancouver Community Network, wrote a blog for CIRA called Vancouver's internet is not for everyone. Broaden it out to include internet access across the country and the same can be said of Canada's internet. It's not currently for everyone because not everyone has access to the social, economic and cultural benefits it provides.

Many things affect access including a lack of infrastructure, the high prices Canadians pay and that some Canadians don't have or can't afford an internet-connected device.

According to the Organisation for Economic Co-operation and Development (OECD), a high-end internet package on a fixed broadband connection (defined as having at least 200 GB/month of data allowance at speeds of at least 25 Mbp) in Canada is $53.26 while the OECD average is $34.17 [19]. Unfortunately, this high price means some Canadians must sacrifice other parts of their budget, namely food[20], in order to pay their internet bills.

For those Canadians who don't own or can't access a device, such as a mobile phone, tablet or computer, while the internet may be available to them, they can't use it.

As Axelsson noted in her blog, "Despite the gigabyte fiber cables beneath their feet, the ultra-fast coffee shop Wi-Fi and the plethora of mobile devices around them, many people are cut off from the jobs, opportunities and connections enabled by the internet. In cities like Vancouver, and dozens of others across Canada, it's not vast geographic distances that keep people offline, it's the inability to connect to the wires and networks that are already there."

Very few Canadian internet users say issues relating to internet cost and access are of little concern to them and six in ten say that internet access should be considered a fundamental right necessary

[19] 4.10 OECD fixed broadband basket, high user, June 2017, https://www.oecd.org/sti/broadband/broadband-statistics/

[20] How the internet feeds hungry Canadians, CIRA, December 2018, cira.ca/food

to the quality of life of all Canadians. In fact, nearly 70 per cent believe the high cost of internet services, including mobile data, is hurting Canada's economy and prosperity.

Percentage of respondents who agree with the following statements

69%
THE HIGH COST OF INTERNET SERVICES, INCLUDING FOR MOBILE DATA, IS HURTING CANADA'S ECONOMY

66%
INTERNET ACCESS SHOULD BE CONSIDERED A FUNDAMENTAL RIGHT NECESSARY TO THE QUALITY OF LIFE OF ALL CANADIANS

18%
ISSUES RELATING TO INTERNET COST AND ACCESS ARE OF LITTLE CONCERN TO ME

CIRA's report *The gap between us: Perspectives on building a better online Canada*[21] details concerns around a lack of infrastructure in remote and rural areas and inequities in digital access and literacy. Report participants also expressed frustration that a handful of players hold the power and receive much of the funding needed to address these issues.

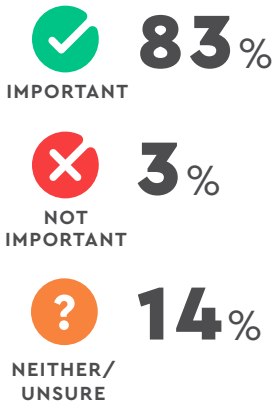
With only a few telecommunications companies in Canada providing the bulk of internet services to Canadians, this lack of competition is a strong contributor to the high prices Canadians pay.

CANADIANS WANT ACTION ON ACCESS

Canadians want more action taken to improve internet access. Seven in ten Canadian internet users agree that the Canadian government should be doing more to support public access to high-speed internet and eight in ten say that universal access to high-speed internet is important for Canada's overall economic growth and prosperity.

[21] The gap between us: Perspectives on building a better online Canada, June 2018, cira.ca/gaps

Importance of universal access to high-speed internet for Canada's economic growth/prosperity



The Canadian government is growing its investments. The Connect to Innovate program will invest $500 million by 2021, to bring high-speed internet to 300 rural and remote communities in Canada[22]. But bringing connectivity to rural and remote communities is not enough. Other solutions that can bring content closer to communities must be explored as well.

For example, CIRA is working with partners to launch an IXP in Iqaluit[23]. This project includes innovative ways to ensure there is a cache of local content available, including everything from security software updates to the ability to stream online TV shows. This will make it easier and faster for locals to access content, as it decreases the reliance on slow and expensive satellite connections.

What other innovations are out there that Canada can tap into to address internet access and quality in remote regions of the country?

Programs like the Government of Canada's Connecting Families, an initiative investing $13.2 million over five years to help bridge the digital divide for Canadian families struggling to afford home internet access , is another example of support.[24] However, single Canadians, including vulnerable seniors, are notably absent from this support.

[22] Connect to Innovate, from Innovation, Science and Economic Development Canada, https://www.ic.gc.ca/eic/site/119.nsf/eng/home

[23] Building, not just bringing, the internet to Iqaluit, Jacque Latour, CIRA blog August 2018, https://cira.ca/blog/state-internet/building-not-just-bringing-internet-iqaluit

[24] Connecting Families, from Innovation, Science and Economic Development Canada, https://www.ic.gc.ca/eic/site/111.nsf/eng/home

Just as digital and media literacy can help Canadians identify fake news online, a lack of digital literacy is also an impediment to access for Canadians who may have a device and internet access, but don't have the skills to benefit from all the internet offers.

The Canadian government's Digital Literacy Exchange Program[25] is one initiative that will help, where $29.5 million will support fundamental digital literacy skills for Canadians who would benefit from participating in the digital economy.

Investments in supporting those without internet access and to enhance digital literacy skills must continue, but addressing other issues, including a lack of competition in Canada's internet services industry, must also be reviewed and action taken.

Canadians overwhelmingly agree – Canada's economy and prosperity is at stake.

[25] Digital Literacy Exchange Program, from Innovation, Science and Economic Development Canada, http://www.ic.gc.ca/eic/site/102.nsf/eng/home

V. INTERNET GOVERNANCE

Given the dichotomy between Canadians' desires and actions online, one can hypothesize a lack of full understanding about how the internet works. The facts grow even clearer, however, when looking specifically at internet governance.

Most Canadians admit that they only know a little (31 per cent) or hardly anything (45 per cent) about the topic of global control and regulation of the internet. In other words, three-quarters of Canadians don't understand the technology that has become the centre of so much of their daily life.

Level of knowledge about global control/regulation of the internet

18%
A LOT/A FAIR AMOUNT

75%
A LITTLE/HARDLY ANYTHING OR NOTHING AT ALL

7%
UNSURE

Given the lack of understanding about how internet governance works today, how can Canadians have a say in the future of Canada's internet? With the divergence between the internet of the West and the internet of the East, combined with the increased security and privacy threats, the risks are greater than ever.

CIRA is concerned about this, and Canadian internet users show concern as well with half expressing worry that the global internet could fracture into regional blocks that adopt very different regulatory principles and policies.

Level of concern that the global internet could fracture into regional blocks

Net neutrality is a prime example of how easily change can happen. Two-thirds of Canadian internet users say they support the principles of net neutrality, and currently, the Government of Canada remains firm in its support of it. Nevertheless, all it takes is an emboldened opposition group to act – right time, right place – for all of it to change, as it did in the U.S. in late 2017.

"The internet ecosystem includes many players: the Canadian Internet Registration Authority (CIRA) and others in the domain industry, content providers, small and medium sized internet service providers, and both non-profit and for-profit value creators including Google. The telecommunications industry is but one player, albeit a powerful one, in a diverse ecosystem. The vast majority of the internet community believe in net neutrality principles and with one bad decision, the majority of the community is put aside for the benefit of one," noted Byron Holland, CIRA's president and CEO in a blog post published in December 2017[26], about the repeal of net neutrality in the U.S.

When asked what Canadians can do to protect net neutrality, Holland encouraged Canadians to stay attentive. "Canadians cannot remain silent, or get too comfortable. The internet we have today can be gone tomorrow if we are not vigilant. Stay informed, engaged and let your voice be heard.[27]"

Knowledge about the internet and how it is governed must be part of that vigilance.

[26] FCC's decision on net neutrality a cautionary tale for Canadians, Byron Holland, CIRA president and CEO, https://cira.ca/blog/state-internet/fcc%E2%80%99s-decision-net-neutrality-cautionary-tale-canadians

[27] The dark side may have won on net neutrality, but there is always a new hope, Byron Holland, CIRA president and CEO, https://cira.ca/blog/state-internet/dark-side-may-have-won-net-neutrality-there-always-new-hope

GROWING KNOWLEDGE ON INTERNET GOVERNANCE IN CANADA

Organizations actively engaged in internet governance have a responsibility to Canadians to spread that knowledge. Understanding how the internet works is a fundamental first step. Understanding who the players are, their motivations and their perspectives, comes next. Lastly, understanding the evolving issues around the internet is also key.

At the United Nations Internet Governance Forum (IGF) in Paris in November, 2018, French President Emmanuel Macron launched the Paris Call for Trust & Security in Cyberspace[28], appealing for greater collaboration between states, the private sector and civil society to improve cybersecurity while protecting citizens' rights online. As of the publication of this report, more than 50 nations and over 450 organizations have signed the agreement, including Canada.

This is a positive development in the world of internet governance, putting cybersecurity at the front of global issues of concern. However, Macron went further than the Paris Call, advocating for increased involvement of governments, including greater government regulation of many elements of the online space to counter misinformation and fake news, online abuse and harassment and other harmful activity.

This begs the question – will this call for increased state involvement counteract the insidious activity Macron seeks to block? Alternatively, does it play into the hands of governments who've long called for multilateral control of the internet, including Saudi Arabia, China, Iran and Russia?

Power can shift. Controls can be tightened. Rights can be lost.

The Paris Call was a key moment that made barely a ripple in major media news outlets in Canada. It's unlikely that most Canadians have even heard about it, nor that they understand the power plays taking place behind the scenes of the internet they know and love. This lack of knowledge opens

[28] Paris Call for Trust and Security in Cyberspace, 12 November, 2018, https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_cyber_cle443433-1.pdf

Canada's internet up to risks that these shifts can occur when no one is looking.

CIRA participates in various fora for multistakeholder internet governance, largely through the IGF and the Internet Corporation for Assigned Names and Numbers (ICANN). Canadian organizations like CIRA, and others who actively participate in internet governance, must rise to the challenge to educate Canadians, helping them to act quickly should changes begin to occur that they disagree with.

CONCLUSION AND RECOMMENDATIONS

1. To counter the spread of fake news:

a. Social media companies must take responsibility to remove content and accounts promoting misinformation online. CIRA's research shows that Canadians favour government regulations/fines for social media companies that do not act to remove content/sites promoting misinformation online.

b. Traditional media sources, including newspapers, TV broadcasters and radio remain among the most trusted sources of information/news in Canada. Canadian journalists therefore have a key role to play in countering fake news that is spreading online. This will be especially important leading up to the federal election.

c. Canadian citizens must be better skilled at recognizing fake news online. Continued investments and resources in digital and media literacy is needed, as well as increased awareness among Canadians about fake news.

2. To enhance the online privacy of Canadians:

a. Canadians have expressed a willingness to pay more for online products/services that protect their data/personal information. Businesses should consider tapping into this to counter the costs of enhancing protections or to lessen reliance on income from advertisers. However, Canadians who say they are willing to pay for privacy must also action that willingness when faced with a dollar amount.

b. Canadian businesses need to better understand Canadian privacy laws and they must follow them.

c. Governments, enterprises and Canadian ISPs need to invest in Canadian infrastructure, such as internet exchange points and cloud services based in Canada in order to keep as much data within our borders as possible. In particular, the Government of Canada, as well as Canada's largest telecommunications companies should be peering at a Canadian IXP.

3. To enhance cybersecurity:

a. Regulation is needed on data collected through IoT devices.

b. The government (federal and provincial) must invest more in helping businesses to be cyber secure, and businesses need to prioritize cybersecurity.

c. Employees and individual Canadians need to grow their knowledge of cybersecurity, including spotting and evading personal attacks, such as phishing emails.

4. To improve internet access:

a. The Canadian government and others must continue to invest in infrastructure and programs ensuring universal internet access across the country, particularly in remote regions and among marginalized Canadians.

b. The internet community and Canadian government must address the internet services oligopoly currently in place in Canada and its impact on the high costs of internet services here.

c. Innovations that bring content closer to internet users must be explored to ensure higher quality internet is available for citizens living in rural and remote communities. A connection alone is not enough.

5. To ensure a safe, secure, open internet in Canada:

a. Organizations engaged in global internet governance must engage Canadians on how internet governance works.

b. Canadians need to grow their knowledge about emerging issues taking place related to internet governance, regulations and controls.

c. Canadians must also take responsibility to stay informed and express their opinions when it comes to Canada's internet, how it's governed and what they want/need.

ABOUT CIRA AND THIS REPORT

CIRA is a member-based, not-for-profit organization, which manages the .CA internet domain on behalf of all Canadians, develops and implements projects that support Canada's internet community and represents the .CA registry internationally. The CIRA team operates one of the fastest-growing country code top-level domains (ccTLD), a high-performance global DNS network, and one of the world's most advanced back-end registry solutions. CIRA participates in various fora for multistakeholder internet governance, largely through the UN Internet Governance Forum (IGF) and the Internet Corporation for Assigned Names and Numbers (ICANN).

CIRA contracted the research firm The Strategic Council to conduct research on issues relating to the Canadian internet in advance of the Canadian Internet Governance Forum 2019. An online panel methodology was used to survey n=1,269 Canadian internet users (18+) between December 20, 2018 and January 2, 2019. The total sample is proportionate to population by gender, age and region.

The survey focused on Canadians' views and experiences around fake news and social media, digital privacy, cybersecurity, internet access and internet governance. Additional information has been referenced and cited throughout this report.