Research Program
on Digital Constitutionalism
Project Aristotle

Canada

Country Report

December 2021

Authors

Angelina Dash, GNLU Centre for Law and Society
Aniket Panchal, GNLU Centre for Law and Society
Bhavnish Kaur, GNLU Centre for Law and Society
Rashi Rawat, GNLU Centre for Law and Society

Institute
for Internet &
the Just Society

project
Aristotle

Research Program on Digital Constitutionalism **Project Aristotle**

Canada

Country Report

Authors
Angelina Dash, GNLU Centre for Law and Society
Aniket Panchal, GNLU Centre for Law and Society
Bhavnish Kaur, GNLU Centre for Law and Society
Rashi Rawat, GNLU Centre for Law and Society

December 2021

Inquiries may be directed to digitalgovdem@internetjustsociety.org

DOI: 10.5281/zenodo.5792093

About us

The Institute for Internet & the Just Society is a think and do tank connecting civic engagement with interdisciplinary research focused on fair artificial intelligence, inclusive digital governance and human rights law in digital spheres. We collaborate and deliberate to find progressive solutions to the most pressing challenges of our digital society. We cultivate synergies by bringing the most interesting people together from all over the world and across cultural backgrounds. We empower young people to use their creativity, intelligence and voice for promoting our cause and inspiring others in their communities. We work pluralistically and independently. Pro bono.

Project Aristotle is the flagship project of the Digital Constitutionalism cycle of the Institute for Internet and the Just Society. Together with our international partners, we publish a research guide on what a structure of governance for the digital realm can look like when it is informed by interdisciplinary country-specific legal and policy research and analysis. We believe that delving deep into these bodies of knowledge, as shaped by a people within a particular national context, has much to offer in response to the pressing questions posed by the digital ecosystem.

Introduction

One of the main focuses of Trudeau government has been to renew Canada's policy framework for the digital age has been internet governance, beginning with foundational principles laid down in Canada's *Digital Charter*.[1] This is a dynamic time for Canadian internet governance. Bills have been proposed to amend the *Broadcasting Act* dealing with the issue of Canadian content online and *Consumer Privacy Protection Act*. Updates to the *Digital Charter* and its *Implementation Act* has been introduced. These bills demonstrate an elevated willingness to act on internet governance issues by the government. They come at a time when, because of the pandemic, the role of internet has been elevated. It is important for people to bring online activity under scrutiny and increase awareness of internet-related issues.

In light of this, the present report discusses the themes of digital Constitutionalism, human rights, privacy and intermediary regulation in a Canada-specific context. Section A will aim at defining digital Constitutionalism and its core tenets for Canada. It will try to present a constitutional model which addresses the concerns and issues with regulating the digital sphere along with being grounded in ideals. The need for an inclusive, representative and equal online spaces has been highlighted. What is analysed here are different sectors in which internet can have a huge role — open source intelligence techniques, competition law, grassroot and judicial actors. It compares the digital and traditional governance model to emphasise on the need for a better legislative space while also considering how diverse national frameworks can come into play for a global digital Constitutionalism

Section B covers human and Constitutionally guaranteed rights. First, it lists out the rights affected by online platforms which fundamentally includes Right to privacy, Right to freedom of expression and Right to equality. Second, the impact of netizens in digital space has been discussed. The discussion extends to the capability of netizens being bad actors. Thereafter, a few approaches have been suggested that could be embedded within the digital ecosystem to cater to the needs of various minorities. Further, an appropriate digital age of consent in Canada has been deliberated upon followed by a discussion on the definition of public order in digital space. Then, it has been analysed if the states should really be allowed to impose censoring practices such as internet shutdowns, slowdowns and communication throttles. The possible socio-legal rational that could be adopted by the states has also been culled out. Lastly, the Social Media Councils (hereinafter, SMC) Model has been expounded within the context of digital Constitutionalism.

Section C mainly deals with Privacy, Information Security and Personal Data in the Canadian context. First, it covers definition of personal data and non-personal data under the laws of Canada. Second, it talks about the ethical, social and economic considerations while dealing with non-personal information. Third, it delves into the end to 'end encryption framework' in Canada wherein the drawbacks of end to end encryption are also discussed in detail. Fourth, the section addresses one of the most important issues of Data Protection in the context of a pandemic; Compliance with Data Protection and Privacy Statutes in times of Crises. Fifth, it discusses regulatory sandboxes, and the grounding philosophy to shape the rules of control for such ecosystems. Lastly, it talks about the principles and regulations as per which intelligence agencies should operate online.

Section D deals with intermediary regulations. It starts off by pointing out the online harms of the internet and highlights the need for drafting, dissemination and enforcement of community guidelines. It covers social media regulation and liability as well as the liability of online platforms concerning user generated content. There should be clear parameters to define problematic user generated content and there is need to moderate fake news. Fundamental rights and safe harbour protection should be balance in order to provide the optimal regulatory space for social media and other internet platforms. Going from a traditional to digital model would require a proactive approach towards understanding and regulating technology in the global intermediary ecosystem. Internet governance can be improved by designing moderation fallibility and guidelines, governance of user-generated content and online advertisement standards. The analysis under the above-mentioned themes is followed by a brief conclusion to the report.

[1] 'Canada's Digital Charter: Trust in a Digital World' (*Government of Canada*, 21 January 2021) <https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html> accessed 10 April, 2021 [hereinafter "Digital Charter"].

A. Digital Constitutionalism and Internet Governance

Introducing Digital Constitutionalism

1. What factors can be considered important to ground Digital Constitutionalism in traditional constitutional concepts?

Canada was established by the British North America Act, 1867 (*Constitution Act*, 1867) and obtained legislative autonomy through the enactment of the *Constitution Act*, 1982 which patriated Canada's *Constitution*. The acts of 1867 and 1982 constitute the Canadian *Constitution* and are the supreme law of the country.[2] The *Constitution* embodies written as well as unwritten principles which reflect its traditional concepts.

The written principles include the Canadian *Charter of Rights and Freedoms*, which guarantees certain rights to citizens, a democratic government and fairness in the justice system.[3] The Supreme Court has outlined the following as unwritten principles:[4] (1) the rule of law; (2) federalism; (3) democracy; (4) protection of minorities; (5) judicial independence; and (6) separation of legislative, executive, and judicial powers. Digital Constitutionalism should be based on these principles. It should safeguard fundamental rights such as freedom of expression, right to privacy, and right to information, and should also protect democracy and rule of law.

Canada released its *Digital Charter* in 2018, with the goal of "better understanding how Canada can drive digital innovation, prepare Canadians for the future of work, and ensure they have trust and confidence in how their data is used."[5] The *Digital Charter* lays down ten principles which will shape Canada's future policy in the digital sphere.[6] It aims to bolster internet access and connectivity for Canadians[7], keeping them safe and secure from the threats of the internet[8] and building a privacy system based on consent, control, and transparency of data[9]. The *Digital Charter* can be understood to be the driving agent for digital Constitutionalism in Canada.

2. How can we define Digital Constitutionalism?

Digital Constitutionalism adapts the core constitutional values to the needs of the digital society.[10] It should extend to private actors too and therefore, include within its purview statutes, regulations, and policies by governments, as well as internal norms and rules set by the companies.[11]

The *Charter of Rights and Freedoms* provides individuals with the right to be secure against unreasonable search or seizure.[12] This includes the right to protection of personal information.[13] The *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) provides that organisations should obtain consent before or at the time that they collect personal data. It is an offence in Canada to intercept private communications or computer systems without express or implied consent.[14]

---

[2] 'Canadian Constitution' (*Government of Canada*, 16 October 2017) <https://www.justice.gc.ca/eng/csj-sjc/just/05.html> accessed 10 July 2021.

[3] 'Guide to the Canadian Charter of Rights and Freedoms' (*Government of Canada*, 8 June 2020) <https://www.canada.ca/en/canadian-heritage/services/how-rights-protected/guide-canadian-charter-rights-freedoms.html> accessed 10 April 2021.

[4] *Reference re Secession of Quebec*, [1998] 2 SCR 217 DLR (4th) 385.

[5] 'Canada's Digital Charter in Action: A Plan by Canadians, for Canadians' (*Government of Canada*, 23 October 2019) <https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00109.html> accessed 10 April, 2021 [hereinafter "Canadian Digital Charter in Action"]

[6] 'Canada's Digital Charter: Trust in a Digital World' (*Government of Canada*, 21 January 2021) <https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html> accessed 10 April, 2021 [hereinafter "Digital Charter"].

[7] 'High-Speed Access for All: Canada's Connectivity Strategy' (*Government of Canada*, 16 July 2019) <https://www.ic.gc.ca/eic/site/139.nsf/eng/h_00002.html#b> accessed 10 April, 2021.

[8] National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age' (*Public Safety Canada*, *Government of Canada*, 28 May 2019) https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx> accessed 10 April, 2021.

[9] 'The Personal Information Protection and Electronic Documents Act (PIPEDA)' (*Office of Privacy Commissioner of Canada*, 11 February 2021) <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/> accessed 10 April 2021; *Privacy Act*, R.S.C., 1985, c. P-21.

[10] Edoardo Celeste, 'Digital constitutionalism: Mapping the constitutional response to digital technology's challenges' (2018) HIIG Discussion Paper Series 2018-02 <https://ssrn.com/abstract=3219905> accessed 10 April 2021.

[11] ibid.

[12] *Digital Charter* (n 5) at section 8.

[13] Leonard Glickman and Sarah Robertson 'Law and the Internet' (*Canadian Encyclopedia*, 2 February 2012) <https://www.thecanadianencyclopedia.ca/en/article/internet-law-and-the#:~:text=In%20Canada%2C%20a%20number%20of,Act%20and%20the%20TRADEMARKS%20Act.&text=The%20Criminal%20Code%20contains%20a,to%20conduct%20on%20the%20Internet> accessed 10 April 2021.

[14] *An Act respecting the Criminal Law*, R.S.C., 1985, c. C-46, s. 184, 342.1

Digital Constitutionalism adapts core constitutional values to the needs of the digital society. Therefore, it must be defined keeping in mind the principles of the *Constitution* as well as the *Digital Charter*. Beyond the *Constitution*, there is also a need for an increased focus on the relationship of individuals with private players. Digital Constitutionalism should encompass public-private policy regimes in online platform regulation, which can also be called co-regulation or shared governance.[15] Online harms caused by violent, offensive, or extremist content should be addressed. The definition should include internal norms of platforms to regulate their content. Technological developments should be integrated into the legal framework to modernize it and address challenges like monopoly, taxation, and workers' rights.

Digital Constitution

3. What should be the core tenets of a Digital Constitution?

Considering these factors, the following ten principles laid down in Canada's *Digital Charter* can be considered the core tenets of digital Constitutionalism[16]:

1. Universal Access

The concentration of most of the population in urban areas makes it a challenge for the government to provide the same internet connectivity to rural communities. The government has launched programs such as High-Speed Access for All,[17] Connect to Innovate,[18] and Digital Literacy Exchange.[19]

2. Safety and Security[20]

To protect individuals from digital risks, the legal framework needs to address privacy and cybersecurity. In addition to the safeguards present in *PIPEDA* and the *Criminal Code* of Canada, the government has also launched the National Cyber Security Policy in 2018.[21]

3. Control and Consent

Along with the consent-based regime of *PIPEDA*, there is a need for tools like data portability which give consumers more control over their information.[22] New frameworks are required for the ethical use of data.[23]

4. Transparency, Portability, and Interoperability

The three guiding pillars[24] for the *Privacy Act* should be respecting and valuing personal information; supporting efficient, adaptable, and innovative approaches to governance; and demonstrating meaningful and transparent accountability.

5. Open[25] and Modern Digital[26] Government

Built on the pillars of transparency and accountability, Canada's open government policy includes the proactive release of and access to federal data and is based on strong information management practices. Canada introduced the 2018–20 National Action Plan on Open Government built on its three previous plans and co-created with public and key stakeholder groups.[27]

6. A Level Playing Field

---

[15] Tarleton Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (Yale University Press 2018).
[16] *Canadian Digital Charter in Action* (n 5).
[17] *High-Speed Access for All: Canada's Connectivity Strategy* (n 6).
[18] 'Connect to Innovate' (*Government of Canada*, 29 May 2020) <https://www.ic.gc.ca/eic/site/119.nsf/eng/home> accessed 10 April, 2021
[19] ibid.
[20] 'Strengthening Privacy for the Digital Age' (*Government of Canada*, 21 May 2019) <https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html> accessed 10 April 2021.
[21] *National Cyber Security Strategy* (n 7).
[22] Teresa Scassa, 'Why Canada needs a national data strategy' (*Policy Options*, 15 January 2019) <http://policyoptions.irpp.org/magazines/january-2019/why-canada-needs-a-national-data-strategy/> accessed 10 April 2021.
[23] ibid.
[24] 'Modernizing Canada's Privacy Act' (*Ministry of Justice*, 15 February 2021) <https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/modern.html> accessed 10 April 2021.
[25] 'Directive on Open Government' (*Government of Canada*, 9 October 2014) <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=28108> accessed 10 April, 2021.
[26] 'Digital Government' (*Government of Canada*, 26 November 2020) <https://www.canada.ca/en/government/system/digital-government.html> accessed 10 April 2021.
[27] 'Canada's 2018-2020 National Action Plan on Open Government' (*Government of Canada*, 9 October 2020) <https://open.canada.ca/en/content/canadas-2018-2020-national-action-plan-open-government> accessed 10 April 2021.

PIPEDA, a key element of Canada's marketplace framework, must also contribute to achieving an inclusive digital economy that provides a level playing field, fairness of opportunity, enhanced security and privacy, predictability for business, and international competitiveness.[28]

7. Data and Digital for Good

The Government of Canada will ensure the ethical use of data to create value, promote openness, and improve the lives of people — at home and around the world.

8. Strong Democracy

To protect Canada's democratic institutions, the government has recognised four pillars:[29] enhancing citizen preparedness against foreign and malicious actors on online platforms; improving organisational readiness and coordination amongst government departments and agencies; combatting foreign interference in the election process; and acting against disinformation, confusion, and exploitation of existing social tensions on the part of social media platforms.

9. Free from Hate and Violent Extremism

Canada has joined many other nations in answering the 'Christchurch call to action' and vowing to eliminate violent extremist and terrorist content online. In line with this, various initiatives have been launched by Canada to meet its commitments: the National Strategy on Countering Radicalization to Violence,[30] the Community Resilience Fund[31], and the Digital Citizen Initiative.[32]

10. Strong Enforcement and Real Accountability

There will be clear, meaningful penalties for violations of laws and regulations that support these principles. To implement the *Digital Charter*, the government has tabled the *Digital Charter Implementation Act*, 2020 to strengthen privacy protections for Canadians.[33]

4. How can Digital Constitutionalism present a Constitutional model for the people, by the people, and of the people?

The emergence of the internet has made consultation among citizens, stakeholders, and governments easier and more equitable.[34] A model of digital Constitutionalism should be developed by involving more people in policymaking. Increasing access to the internet can further citizen awareness and ensure that they make their issues heard by getting support online. Further, an open government policy will improve access to information. It facilitates making informed decisions because information from all viewpoints is available. Information should be accessible in the most equitable manner and online platforms or governments should not exert their control on the content that is available to the public. Digital Constitutionalism should be for the people wherein the policy is aimed at regulation of hate content, violent extremism, data breaches, and monitoring/surveillance of citizens' data.

The following examples from Canada show how citizens' involvement has been considered by the government for formulating their approach towards the digital economy. Canada's first ever digital economy strategy, Digital Canada 150 (DC 150), was launched in 2014 after holding consultations with people and the private sector.[35] The Open Government Initiative launched by Canada in 2011 engaged citizens, private sector, civil society, and other levels of government.[36] More recently, Canada's *Digital Charter* involved stakeholders at every step of the way. In 2016, the Innovation and Skills Plan was introduced to foster

[28] *Strengthening Privacy for the Digital Age* (n 20).
[29] 'Protecting democracy' (*Government of Canada*, 19 March 2021) <https://www.canada.ca/en/democratic-institutions/services/protecting-democracy.html> accessed 10 April 2021.
[30] 'National Strategy on Countering Radicalization to Violence' (*Public Safety Canada*, 11 December, 2018) <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-strtg-cntrng-rdclztn-vlnc/index-en.aspx> accessed 10 July 2021.
[31] 'Community Resilience Fund' (*Public Safety Canada*, 17 April 2014) <https://www.publicsafety.gc.ca/cnt/bt/cc/fnd-en.aspx> accessed 10 July 2021.
[32] 'Online Disinformation' (*Government of Canada*, 30 June 2021) <https://www.canada.ca/en/canadian-heritage/services/online-disinformation.html> accessed 10 July 2021.
[33] 'Bill summary: Digital Charter Implementation Act, 2020' (*Government of Canada*, 23 November 2020) <https://www.ic.gc.ca/eic/site/062.nsf/eng/00120.html> accessed 10 April 2021.
[34] Justin Longo, 'The evolution of citizen and stakeholder engagement in Canada, from Spicer to #Hashtags' (2017) 60(4) Canada Public Administration 517 <https://onlinelibrary.wiley.com/doi/full/10.1111/capa.12229> accessed 10 April 2021.
[35] 'Digital Canada 150: Canada's digital "strategy"' (*Circa*, 4 April 2014) <https://www.cira.ca/fr/blogue/state-internet/digital-canada-150-canadas-digital-strategy> accessed 10 July 2021.
[36] *Justin Longo* (n 34).

innovation in the country.[37] In 2018, the National Digital and Data consultations were launched in order to understand the public's views about how the digital age affects them. The principles laid down in Canada's *Digital Charter* are drafted on the basis of the consultation that the government had with its citizens. It lays down the most important issues facing people and comes up with ten principles forming the "building blocks of a foundation of trust for this digital age."[38]

Representativeness of Online Platforms

5. How can online platforms be made more inclusive, representative, and equal?

The concerns around online platforms deal with the ability of citizens to exercise their freedom of expression, presence of diversity, and civic engagement.[39] First, freedom of expression is threatened by online trolls and bots which spread hate content. Censorship or distortion by governments and online platforms further curtails freedom of expression. Second, the monopolistic nature of certain online spaces impacts diversity of content available as well as cultural representation online. Third, foreign intervention in elections threaten democracy and creation of echo chambers makes civic engagement across ideological lines difficult.

1. Diversity of content online[40]

Diversity of content is important to expose citizens to a wide range of views and perspectives. It promotes healthy public discourse, encourages tolerance, fosters greater social inclusion, and builds citizens' resilience to disinformation.

For this purpose, a multi-stakeholder working group has been formed in 2018 under the Department of Canadian Heritage's International Engagement Strategy on Diversity of Content.[41] The principles developed by the group would be centred around four themes: (1) creation, access, and discoverability of diverse content online; (2) fair remuneration and economic viability of content creators; (3) promotion of reliable information and building resilience against disinformation; and (4) transparency of the impacts of algorithmic treatments of online content.[42]

2. Regulation of Social Media Platforms[43]

The Department of Innovation, Science and Industry is addressing privacy and data issues through Canada's *Digital Charter* and enhanced powers for the Privacy Commissioner. Global Affairs Canada addresses foreign interference through the G7 Rapid Response Mechanism, and Public Safety Canada addresses violent and extremist content online through its Canada Centre for Community Engagement and Prevention of Violence and through engagements in the Global Internet Forum to Counter Terrorism (GIFCT) and the Five Country Ministerial.

The Government is committed to introducing new regulations for social media platforms, starting with a requirement that all platforms remove illegal content, including hate speech, within 24 hours. Other online harms in scope include radicalization, incitement to violence, the exploitation of children, and the creation or distribution of terrorist propaganda. After calls from Canadians about the need for more robust regulation of social media, the federal government has plans to introduce legislation imposing obligations on internet platforms to remove unlawful speech.[44]

---

[37] 'Innovation for a better Canada' (*Government of Canada*, 2 June 2020) <https://www.ic.gc.ca/eic/site/062.nsf/eng/home> accessed 10 April 2021.

[38] *Canadian Digital Charter in Action* (n 5).

[39] Eileen Donahoe and Fen Osler Hampson (ed), *Governance Innovation for a Connected World Protecting Free Expression, Diversity and Civic Engagement in the Global Digital Ecosystem* (Centre for International Governance Innovation, 2018) <https://www.cigionline.org/sites/default/files/documents/Stanford%20Special%20Report%20web.pdf> accessed 10 April 2021.

[40] 'Diversity of content online' (*Government of Canada*, 26 February 2021) <https://www.canada.ca/en/canadian-heritage/services/diversity-content-digital-age.html> accessed 10 April 2021.

[41] 'International Engagement Strategy on Diversity of Content Online' (*Government of Canada*, 8 February, 2021) <https://www.canada.ca/en/canadian-heritage/services/diversity-content-digital-age/international-engagement-strategy.html> accessed 10 July 2021.

[42] *Diversity of content online* (n 40).

[43] 'Regulation of social media Platforms' (*Government of Canada*, 10 December 2020) <https://search.open.canada.ca/en/qp/id/pch,PCH-2020-QP-00084> accessed 10 April 2021.

[44] Sonja Solomun, Maryna Polataiko and Helen A. Hayes 'Platform Responsibility And Regulation In Canada: Considerations On Transparency, Legislative Clarity, And Design' (2021) 34 Harv. J.L. & Tech. 1 <http://jolt.law.harvard.edu/assets/digestImages/Solomun-Polataiko-Hayes.pdf> accessed 10 April 2021.

6. What role should open-source intelligence (=OSINT: the discipline of assembling and analyzing publicly available information) play in the future of our society?

Open-source intelligence techniques (OSINT) have been very useful for security consultants, scientists, and media as well as the intelligence community. With the increased availability of personal open source information on the internet, the role that OSINT plays will only increase. To use it effectively, it is important for governments to tackle the challenges that come with it. It can lead to the construction of virtual personal identities by others,[45] facilitate more social control by the state,[46] and raise significant privacy and data protection concerns for the public.[47]

The Rapid Response Mechanism (RRM) Canada has laid down an ethical and methodological framework for open source data monitoring and analysis.[48] This was done to ensure that data monitoring activities are politically neutral, respect and reinforce human rights and freedoms, and comply with relevant legal and regulatory provisions. The framework also provides transparency and accountability to Canadians and the G7. Beyond existing law and policy, it is necessary for principles and ethical considerations to be incorporated into open source data monitoring and analysis.

Open source data should take human rights into consideration. In order to respect the privacy of the citizens, open source data monitoring and analysis should be limited to publicly available data and should be consistent with Canada's privacy laws. Foreign activities with a coercive, corrupt, covert, or malicious dimension that attempts to sway public opinion are a threat to freedom of expression. There is a need to focus on the structure and context of conversations rather than content to effectively identify foreign interference. The Canadian security, intelligence, and law enforcement organisations as well as the Commissioner of Canada Elections should have better information sharing and coordination. No active measures should be taken with content creators or those sharing content. To address equality, inclusion, and representation concerns surrounding open source data, it is important to understand the way malign actors target marginalised groups. The Gender-Based Analysis Plus (GBA+)[49] approach has been recommended by RRM Canada to tackle this problem.

7. Should the Digital Constitution be an integrative model, which draws upon and comprehensively presents standards for specific laws (e.g. antitrust, evidentiary standards etc.) as opposed to grounding ideals? If so, how should it fulfil the responsibilities of a pluralistic enterprise such as this as well as the specific needs of a pluralistic global society?

The approach that Canada is taking in this regard is to modernize their laws in accordance with certain principles laid down in their *Digital Charter released* in 2018.

1. Privacy[50]

The *Digital Charter Implementation Act*, 2020 has been tabled which has the aim of strengthening privacy protections for Canadians as they engage in commercial activities. The *Act* will create the *Consumer Privacy Protection Act (CPPA) and Personal information and Data Protection Tribunal Act*. Finally, the *Act* will repeal Part 2 of *PIPEDA* and turn it into stand-alone legislation, the *Electronic Documents Act*.

2. Intellectual Property[51]

---

[45] E. Morozov, *The Net Revolution: How not to liberate the world* (Penguin Books, 2010).

[46] Quirine Eijkman and Daan Weggemans, 'Open source intelligence and privacy dilemmas: Is it time to reassess state accountability?' (2013) 23(4) Security and Human Rights 285 <https://www.researchgate.net/publication/256057526_Open_Source_Intelligence_and_Privacy_Dilemmas_Is_it_Time_to_Reassess_State_Accountability> accessed 10 April 2021.

[47] ibid.

[48] 'Ethical and methodological framework for Open source data monitoring and analysis' (*Government of Canada*, 13 August, 2019) <https://www.international.gc.ca/gac-amc/publications/rrm-mrr/ethical_framework-cadre_ethique.aspx?lang=eng> accessed 10 July 2021.

[49] 'Gender-based Analysis Plus (GBA+)' (*Government of Canada*, 14 April 2021) <https://women-gender-equality.canada.ca/en/gender-based-analysis-plus.html> accessed 10 July 2021.

[50] *Bill summary: Digital Charter Implementation Act, 2020* (n 33).

[51] Daniel Daniele, 'Canada: The Battle For Copyright Protection In The Digital Era' (*Mondaq*, 14 July 2017) <https://www.mondaq.com/canada/copyright/610524/the-battle-for-copyright-protection-in-the-digital-era> accessed 10 April 2021.

To protect individuals and enforce their intellectual property (IP) rights online, the new legislative regime works through a set of notices. If the owner of a copyrighted work believes that his or her copyright has been infringed, the owner may send a notice of infringement to an internet service provider.[52]

3. Competition[53]

The Competition Bureau has recognised the challenges that come with technology firms and have formulated three supporting pillars for their strategic vision: protecting Canadians through enforcement, promoting competition in Canada, and investing in their organization. The Bureau will be at the forefront of enforcement in the digital economy by addressing anti-competitive practices in the field.

4. Evidentiary standards[54]

The *Uniform Electronic Evidence Act* was enacted in Canada in 1998 as a statutory response to the growing use of digital technology as the primary means of conducting activities and producing records.

5. Online Platforms[55]

Canada is going to come up with legislation to combat hate groups and online hate and harassment.[56] It will apply to online platforms and includes the establishment of a regulator meant to oversee platforms' management of unlawful online speech. The regulator will have the authority to impose financial penalties on platforms for failure to comply.

6. Cyber security[57]

Canada released its new cyber security strategy in 2018. The Canadian Cyber Threat Exchange (CCTX) became operational in 2016 to improve information sharing on cyber threats faced by the private sector. Later in 2018, the Canadian Centre for Cyber Security (CCCS) was established as the government's point of contact with the CCTX.

Digital Constitutionalism should be based on both approaches depending on the nature of the issue to be addressed. In cases where the existing comprehensive regulatory approach can be modified to include aspects of the digital age like competition law, evidentiary standards, and intellectual property, it can be based on an integrative model. However, there are also aspects of emerging technologies which require a complete overhaul in the system since they cannot be incorporated in the present framework.

In this regard, the approach that Canada has taken can serve as a guiding point for other countries as well. Having a digital charter ensures that there are certain basic principles in place to guide the digital governance model. At the same time, it is flexible to either incorporate the challenges of the digital age into existing laws or to create new legislation. A digital charter helps to meet the needs of a pluralistic society by taking all interests into account. It can also be incorporated into pluralistic enterprises as guidance for their internal regulations.

Competition Law and the Internet

8. How can competition and antitrust laws of different jurisdictions protect the global market from big-tech domination, and is there a need to?

In a 2018 study, it was found that Canada has some of the highest levels of competition-stifling regulation among developed economies.[58] The researchers estimate that Canada could see a four to five percent boost in productivity by reforming regulations and reducing barriers to entry. There is a need for competition and

---

[52] *Copyright Act*, R.S.C. 1985, c. C-42, s. 41.26(1).

[53] *Competition in the digital age: the Competition Bureau's strategic vision 2020-24*, (Competition Bureau Canada, 2020) <https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/Strategic-Vision-2020-24-En.pdf/$file/Strategic-Vision-2020-24-En.pdf> accessed 10 April 2021.

[54] Luciana Duranti, Corinne Rogers and Anthony Sheppard, 'Electronic Records and the Law of Evidence in Canada: The Uniform Electronic Evidence Act Twelve Years Later' (2010) 70 Archivaria 95. <https://commons.allard.ubc.ca/cgi/viewcontent.cgi?article=1321&context=fac_pubs> accessed 10 April 2021.

[55] *Sonja Solomun, Maryna Polataiko and Helen A. Hayes* (n 70).

[56] ibid.

[57] Stephanie Carvin, 'Canada and Cyber Governance' (Centre for international Governance Innovation) <https://www.cigionline.org/articles/canada-and-cyber-governance> accessed 10 April 2021.

[58] Gilbert Cette, Jimmy Lopez, Jacques Mairesse 'The impact of regulation on rent creation, rent sharing, and total factor productivity' (*VOX EU*, 13 September 2018) <https://voxeu.org/article/impact-regulation-rent-creation-rent-sharing-and-total-factor-productivity> accessed 10 July 2021.

antitrust laws to address this because, while network effects can bring efficiency and benefits consumers, it is also a huge barrier to entry that may limit competition.[59]

The competition sector needs an overhaul to deal with changes in the digital economy. First, stricter scrutiny on anti-competitive mergers between tech companies is required since the traditional method followed by the Competition Bureau of Canada will not be effective against such firms. Second, while big data can be an output that is sold and priced just as any other good, it can also be an input that is neither sold nor priced. The latter raises issues regarding the applicability of present competition tools and methods. Third, the Bureau should distinguish between deceptive marketing practices related to collection of data and those related to use of data. Fourth, competition law usually concerns effects on price, but the enforcement must also deal with non-price effects as these are relevant in big data cases. For example, users may view privacy as an important component to determine the quality of the service that used big data.

These concerns were recognised by the deputy commissioner of the Bureau[60] and it was acknowledged that in the age of big data, many competition regulations would need to be updated. However, despite the assurance from the Competition Bureau that it was monitoring tech giants for anti-competitive practices, the Bureau's enforcement in the digital sphere has been lacking.[61] The Competition Bureau of Canada has been criticised for taking a softer approach when it comes to enforcement activities against big tech firms.[62] In 2019, the Bureau appointed a Chief Digital Enforcement (CDE) Officer who would advise them on wide range of matters including tools and development in order to strengthen investigations in the digital economy.[63]

Data mobility is important to maintain competition. Because of network effects, switching is becoming less common owing to costs, complications, and inconvenience. Therefore, it is important to increase data portability to allow users to easily transfer their personal data from one platform to another. This will also address concerns around privacy if users can switch providers easily and securely in events of privacy breaches. Interoperability among different platforms is another factor. In Canada, the banking sector is pursuing data mobility through an open banking initiative,[64] and this has also been proposed in the upcoming CPPA.[65] Such an environment will enable conditions that drive competition.

The Regional, Constitutional and Transnational Aspects of a Digital Constitution

9. What is the role of regional/grassroots actors as well as inter-judicial cooperation/coordination in the digital ecosystem? Which other mechanism(s) might be more helpful?

Civil societies like the Global Commission on Internet Governance based in Canada have recommended frameworks that adopt distributed, multi-institutional approaches to the governance of different technical and non-technical internet-related issues.[66] Distributed governance enables cooperation between existing and emerging actors and organisations. A distributed system means interoperability and collaboration within the governance systems.[67] Through a decentralised system and the elimination of bureaucracy, networks will be flexible, fluid, and creative. Distributed governance allows for both granularity (localization) and scale

[59] Competition Bureau, "Big data and innovation: key themes for competition policy in Canada" (19 February 2018) <https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/ eng/04342.html> accessed 10 July, 2021.

[60] Anthony Durocher, 'Competition in the Age of the Digital Giant' (*Government of Canada*, 13 June 2019) <https://www.canada.ca/en/competition-bureau/news/2019/06/competition-in-the-age-of-the-digital-giant.html> accessed 10 April 2021.

[61] Vass Bednar and Robin Shaban, 'Why our toothless competition bureau can't go after the big tech' (*National Post*, 26 March 2021) <https://nationalpost.com/opinion/opinion-why-our-toothless-competition-bureau-cant-go-after-big-tech> accessed 10 April 2021.

[62] ibid.

[63] Mark Katz, 'Recent Developments in Canada: Will the Competition Bureau Intrude on Privacy?' (*Kluwer Competition law*, 24 September 2019) <http://competitionlawblog.kluwercompetitionlaw.com/2019/09/24/recent-developments-in-canada-will-the-competition-bureau-intrude-on-privacy/> accessed 10 April 2021.

[64] 'A Review into the Merits of Open Banking' (*Government of Canada*, 11 February 2019) <https://www.canada.ca/en/department-finance/programs/consultations/2019/open-banking.html> accessed 10 July 2021.

[65] Teresa Scassa, 'Data Mobility (Portability) in Canada's Bill C-11' (12 January, 2021) <https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=338:data-mobility-portability-in-canadas-bill-c-11&Itemid=80> accessed 10 July 2021.

[66] Stefaan G. Verhulst and others, 'Innovations in Global Governance: Toward a Distributed Internet Governance Ecosystem' (2014) Global Commission on Internet Governance Paper series No. 5 <https://www.cigionline.org/sites/default/files/gcig_paper_no5.pdf> accessed 10 April 2021.

[67] ibid.

(globalization) by adopting expert- or issue-based organizing principles that help coordinate decision making on issues across and between the local, national, regional, and global levels.[68]

The courts in Canada have played an important role in upholding rights of users in the digital ecosystem. In a landmark 2017 decision, it was held that courts have the power to order online intermediaries to remove illegal content from their search results.[69] This goes a long way in respecting the IP of copyright holders. Proposals for modernising *PIPEDA* include improved order making, statutory damages and penalty imposing powers of the Courts for violation of obligations under the *Act*.[70] The proposed *CPPA* includes the creation of a Personal Information and Data Protection Tribunal, an administrative tribunal empowered to levy significant fines for non-compliance.[71] The jurisprudence on various sections of the Canadian *Charter of Rights and Freedoms* has developed with a lens wide enough to encompass the changing tides of technology.[72] Right to life, liberty, and security, and the protection against unreasonable search and seizure have been interpreted to cover protection against unreasonable invasions of privacy.[73]

10. Can the Digital Constitution present an anchor for the governance of the virtual world similar to a traditional Constitutional model or will it always be in flux? Is there a need for Constitutional innovation, and if so, in which areas (e.g. the right to be forgotten as a novel right)?

The dynamic nature of the internet and constant innovations in the field mean that the governance framework too should be flexible and ever evolving. Canada has incorporated these principles in its *Digital Charter*, and that can act as the basis of its e-governance approach. A digital Constitution has to be flexible in order to adapt to constant change but also at the same time lay down certain key concepts that will form the root of government action.

The digital revolution is a major human rights issue. Cyberspace and artificial intelligence (AI) should not remain ungoverned.[74] The digital economy brings challenges to freedom of expression and incitement to hatred and violence. Failure to act will result in the further shrinking of the civic space, decreased participation, heightened discrimination, and a continuing risk of lethal consequences — in particular for women, minorities, and migrants, for anyone seen as 'other'. But over-reaction by regulators to rein in speech and the use of the online space also concerns human rights. Dozens of countries are limiting what people can access, curbing free speech and political activity, often under the pretence of fighting hate or extremism. Many countries have done this by imposing internet shutdowns and through other ways of limiting freedom of speech and expression.[75]

There is a need for recognising additional rights in the context of the internet — right to internet neutrality, universal access to the internet, digital security, education and digital protection of minors, rectification in the web, information updates by digital media outlets, privacy and the use of digital devices in the workplace, and those related to unplugging, video surveillance and geolocation in the workplace, digital rights to collective negotiation, not saving browsing history, portability and the digital will.[76]

Historically, Canada has had a good track record for the protection of political rights and civil liberties. However, in recent years, there have been concerns around surveillance laws.[77] The private sector holds data

[68] ibid.

[69] 'Landmark Canadian Supreme Court ruling: Search engines can be compelled to remove illegal sites from results' (CISAC, 28 June 2017) <https://www.cisac.org/Newsroom/society-news/landmark-canadian-supreme-court-ruling-search-engines-can-be-compelled-remove> accessed 10 July 2021.

[70] 'The Case for Reforming the Personal Information Protection and Electronic Documents Act' (*Office of Privacy Commission of Canada*, May 2013) <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_r/pipeda_r_201305/#toc4a> accessed 10 July 2021.

[71] Carole Piovesan, Noel Corriveau and Ellen Xu, 'Canada: Privacy Law For The Digital Economy: The New Digital Charter Implementation Act' (*Mondaq*, 29 November 2020) <https://www.mondaq.com/canada/privacy-protection/1010638/privacy-law-for-the-digital-economy-the-new-digital-charter-implementation-act> accessed 10 July 2021.

[72] R. v. Wong, [1990] S.C.J. No. 118, [1990] 3 S.C.R. 36, at 43-44 (S.C.C.).

[73] *See for eg.*, R v. Spencer, [2014] S.C.J. No. 43, [2014] S.C.R. 212, 2014 SCC 43 (S.C.C.).

[74] Michelle Bachelet, 'Human rights in the digital age' (*United Nations Human Rights office of High Commissioner*, 17 October 2019) <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25158&LangID=E> accessed 10 April 2021.

[75] ibid.

[76] José María Lassalle, 'Digital Citizenship: For a new generation of human rights' (*Open Democracy*, 16 December 2019) <https://www.opendemocracy.net/en/democraciaabierta/ciudadan%C3%ADa-digital-por-una-nueva-generaci%C3%B3n-de-derechos-humanos-en/> accessed 10 April 2021.

[77] 'Freedom on net 2020 – Canada' (*Freedom House*, 2020) <https://freedomhouse.org/country/canada/freedom-net/2020> accessed 10 April 2021.

about individuals such as their physical location, facial features, and behaviour. The use of closed-circuit cameras for surveillance in smart cities also poses concerns. There is a need to extend certain rights to the private sector considering their increasingly pervasive role in the everyday lives of Canadians.[78] The use of cloud computing and web-based email services mean that there is cross border sharing of Canadian data which has privacy and other legal implications. In the last few years, emerging AI in different sectors has been shown to have discriminatory effects.[79]

Therefore, considering the needs of the evolving digital economy, digital Constitutionalism will have to be updated with the human rights challenges of the digital age.

11. How is it possible to harmonise diverse national frameworks in order to achieve a global Digital Constitution?

Serious and complex governance challenges in the areas of surveillance, censorship, privacy, access, and spam are exacerbated as a result of differing national approaches. Issues that affect the technical operation of the internet require global coordination to ensure the internet functions as one coherent system. This requires (and in turn can build) greater trust and transparency among actors. It also requires a greater effort at inclusiveness and a more rigorous use of evidence, data, and case studies to help stakeholders and governments from all countries determine where to turn to address issues within the intricate — and largely fragmented — matrix of internet governance.

Having a multi-stakeholder approach can resolve this problem. There is a gap in the broad framework that countries adopt to cover digital policy issues. This is related to the challenge of lack of trust among governments, civil society, and the private sector. Inter-governmental work must be balanced with work involving broader stakeholders. Multi-stakeholder and multilateral approaches can and do co-exist. The challenge is to evolve ways of using each to reinforce the effectiveness of the other. We need to bring far more diverse voices to the table, particularly from developing countries and traditionally marginalised populations. Important digital issues have often been decided behind closed doors, without the involvement of those who are most affected by the decisions.

The cross-border nature of digital transactions demands national frameworks to multi-jurisdictional privacy and data protection regulations. These regulations need to be compatible with the *European Union's General Data Protection Regulation (GDPR)* and global best practices.[80] The United Nations has identified nine values which can shape the development of digital cooperation.[81] The G20 has proposed a common framework for measuring the digital economy to address key gaps and challenges.[82] The report recommends several steps to create this framework:

1. Establishing a common definition of the digital economy
2. A suite of key indicators for monitoring developments related to jobs, skills, and growth in the digital economy.

B. Human and Constitutionally Guaranteed Rights

Internet Users and Online Platforms

1. Which human and Constitutionally guaranteed rights do online platforms affect, and how?

[78] Aaron Shull, 'The Charter and Human Rights in the Digital Age' (Centre for International Governance Innovation, 16 Aug 2018) accessed 27 March 2021.
[79] ibid.
[80] 'Canada's Economic Strategy Tables: Digital Industries' <https://www.ic.gc.ca/eic/site/098.nsf/vwapj/ISEDC_Digital_Industries.pdf/$file/ISEDC_Digital_Industries.pdf> accessed 10 July 2021.
[81] *The age of digital interdependence: Report of the UN Secretary-General's High-level Panel on Digital Cooperation* (Digital Cooperation: UN secretary General's High Level Panel, 2019) at 7 <https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf> accessed 10 April 2021.
[82] *A Roadmap Toward A Common Framework For Measuring The Digital Economy: Report for the G20 Digital Economy Task Force* (OECD, 2020) <https://www.oecd.org/sti/roadmap-toward-a-common-framework-for-measuring-the-digital-economy.pdf> accessed 10 April 2021.

Today, online platforms undoubtedly influence the way we exercise our basic rights. Although they come with considerable positives, they are numerous opportunities for large-scale violations. The human rights framework of Canada includes, among others, the Canadian *Charter of Rights and Freedoms*[83] and the Canadian *Bill of Rights*.[84]

The fundamental rights recognised in those documents are just as applicable online as offline. In addition to these rights mentioned herein above, there are rights specific to the protection of privacy and personal data[85] and the *Personal Information Protection and Electronic Documents Act*[86] (*PIPEDA*). The rights guaranteed under the above-mentioned laws that are affected by online platforms include collection and use of online personal data by online platforms. The Law contains a set of principles that must be applied to companies when they are processing personal information of an identifiable person.[87] Activities affecting human rights would include the massive monitoring and collection of personal information, in a ubiquitous invasion of privacy.[88] However, apart from the obligations and guidelines stipulated in *Schedule 1 of PIPEDA*, there do not appear to be specific regulations on data protection in respect to social networking, smartphone applications, or geographic data. Nonetheless, a report by Privacy Commissioner stated, "PIPEDA would apply to the personal information handling practices of private sector organizations engaged in online tracking, profiling and targeting, and cloud computing." [89]

Further, Canada's private sector data protection laws are somewhat problematic. *PIPEDA* requires organizations subject to the act to obtain an individual's consent before or at the time that their personal information is collected.[90] However, the reality is that consumers usually scroll through lengthy agreements that describe how their personal information is used. Nor is there a meaningful alternative in many instances — individuals face a 'take it or leave it' proposition.

Other activities affecting guaranteed rights would include techniques to filter content, manage copyright, block access to certain websites, and restrict freedom of expression.[91] Further, anonymity is essential to the exercise of free expression online.[92] However, it has been witnessed that several activists have been disallowed from using pen names on Facebook.[93] Such actions, among others, adversely affect free expression guaranteed by the *Canadian Charter*. Further, the *Canadian Charter* includes fundamental freedoms including the right to equal protection and equal benefit of the law without discrimination. Online platforms could affect these guaranteed rights including the right to equal protection and equal benefit of the law without discrimination through their various actions.

2. Who can be defined as a netizen? [94]

Today, we live in the age of the networked citizen, where to be networked is the defining element of citizens' agency. The word Netizen came into being in the mid-1990s and literally means 'citizen of the internet'. It is believed that the term was coined by Michael Hauben. He used the term to describe the people who inhabit the 'electronic commons' of the internet. Accordingly, it would appear that Netizen, as a term of wide import, would generally encompass any individual who has access to the internet.

At this point, it is of crucial importance to draw a distinction between Netizens and the people who come online merely to use the internet. To put things in perspective, a Netizen could be described as an individual

---

[83] Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, Schedule B to the Canada Act 1982 (UK), c 11, art 1.
[84] Canadian Bill of Rights, SC 1960, c 44.
[85] Privacy Act, RSC 198, c P-21.
[86] Personal Information Protection and Electronic Documents Act, SC 2000, c. 5.
[87] ibid, Sec 2.
[88] Hick, S, Halpin, E and Hoskins, E, dir. *Human Rights and the Internet*, 2000, Palgrave Macmillan, Part IV; DE NARDIS, L. *The Emerging Field of Internet Governance*, Yale Information Society Project Working Paper Series, 2010, p. 11 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1678343> accessed 28 March 2021.
[89] Office of The Privacy Commissioner of Canada, Report On The 2010 Office of The Privacy Commissioner of Canada's Consultations On Online Tracking, Profiling and Targeting, And Cloud Computing (May 2011), <http://www.priv.gc.ca/resource/consultations/report_201105_e.asp>
[90] Aaron Shull, 'The Charter and Human Rights in the Digital Age' (Centre for International Governance Innovation, 16 Aug 2018) accessed 27 March 2021.
[91] Hick, S, Halpin, E and Hoskins, E, dir. *Human Rights and the Internet*, 2000, Palgrave Macmillan, Part IV; DE NARDIS, L. *The Emerging Field of Internet Governance*, Yale Information Society Project Working Paper Series, 2010, p. 11 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1678343> accessed 28 March 2021.
[92] https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx
[93] https://www.opendemocracy.net/en/what-can-social-media-platforms-do-for-human-rights/
[94] Michael Hauben, 'The Net and Netizens: The Impact the Net has on People's Lives' (*Columbia*, 5 June 1996)<http://www.columbia.edu/~rh120/ch106.x01> accessed 15 March 2021.

who actively seeks to contribute to the development of the internet while the same cannot be said for the individuals who merely use the internet. In fact, the second category of individuals are differentiated from the netizens and are popularly known as 'Lurkers'.

Lurkers cannot be said to be a part of the group of Netizens as they do not actively engage or contribute to the internet. Therefore, the predominant differentiating factor between Netizens and Lurkers is an interest and active engagement in the improvement of the internet. Further, the distinct criteria to identify Netizens would include the participation of individuals with an aim to ensure that the internet becomes both an intellectual and a social resource. Netizens are individuals who do not come online for isolated profit or gain. They do not include individuals who think internet is a service and must be consumed for their individual benefit. Rather they are people who consider everyone as their compatriot and are always ready to make efforts and actions in order to make the Internet a regenerative and vibrant community.

The advent of the internet has provided an all-embracing virtual space to the people around the world in order to be intellectually interesting and interested. Net society differs from off-line society by welcoming intellectual activity. People are encouraged to have things on their mind and to present those ideas to the Net. Netizens, thus, interact with other people to help add or alter the information that is being borne in others' minds. Brainstorming by Netizens would result in robust thinking exercises and vigorous exchange of information. Netizens would try and ensure that information does not remain a fixed commodity, rather it should be improved collectively.

Thus, Netizens working together aim to continually expand the horizons of the available information transcending the physical boundaries. This, in turn, unleashes the untapped resources for it provides a suitable alternative to the conventional channels and ways of information exchange. The Net allows for the meeting of minds to form and develop ideas. It brings people's thinking processes out of isolation and into the open. Every user of the Net gains the role of being special and useful. The fact that every user has his or her own opinions and interests adds to the general body of specialised knowledge on the Net. Therefore, each Netizen is a special resource valuable to the internet. Each of them contributes to the whole intellectual, social value and possibilities of the Internet. In light of the foregoing, a netizen can be characterised as an active participant on the internet who considers it to be his/her obligation to make internet a better place than what it has already been so far.

3. Who can be classified as a 'bad actor', and can 'bad actors' be netizens?

Bad actors could be characterised as individuals who become part of unethical activities persisting on the internet such as racism, misogyny, etc. Moreover, bad actors in the digital space are involved in a multitude of illegal and unethical activities such as cyber-attacks, doxing, and trolling. They primarily affect privacy, freedom of speech and user protections of individuals on the internet.[95] Thus, 'bad actors' is a term of a wide import which would also include spammers, harassers and individuals involved in similar activities on the internet. Although a great deal of these activities happens in public view, it is quite worrisome that privacy and safety advocates, in an effort to create a safer and equal space, will push these bad-actors into more-hidden channels. The worst outcome is that we will end up with a kind of cloaked internet in which everything looks reasonably bright and sunny, which hides a more troubling and less transparent reality. Further, our data is often stolen by these bad actors who will also be using machine learning processing to steal or destroy things we value as individuals: our identities, privacy, money, reputations, property, elections, etc.

At this juncture, there arises a perplexing question, whether 'netizens' who uses internet for the benefit of the society be bad actors? Although not an out-and-out satisfying answer, netizens can be characterised as bad actors in certain scenarios. Of course, deliberate troublemakers exist but there are also individuals who believe in their own minds that they are not bad actors at all but are fighting a good fight for all which is right and true. These types of scenarios can also be termed as situations of 'where you stand depends on where you sit'. Therefore, there could be instances where an individual, in his mind thinking that he is being a law-

[95] Wolfgang Kleinwachter, 'Bad Actors Want to Target the Internet's Infrastructure. If That Happens, We're in Trouble' <https://www.brinknews.com/bad-actors-want-to-target-the-internets-infrastructure-if-that-happens-were-in-trouble/> accessed 22 August 2021.

abiding Netizen, still harms the digital space and by extension society because of his misconceptions about his activities.[96]

Safeguarding the Digital Ecosystem: Minority Rights Protection and Consent

4. How can we embed within the digital ecosystem approaches which are responsive to the needs of minorities (e.g. ethnic minorities, racial minorities, gender minorities, religious minorities)?

The 'digital divide' is no longer a dichotomy between who has access to the internet and who does not. The digital divide has evolved into a broader concept including access to digital services, relevance of content, affordability, and education. Factors driving digital exclusion include language, gender, (dis)abilities, age, skillset, and income. Further, as a consequence of this, offline inequalities are being reflected and accentuated in the online environment. For instance, low-income households, minorities, rural populations and women are the most at-risk of digital exclusion.[97] On a global scale, women "are 12% less likely to use the internet." This increases to 50% for people with disabilities.[98] Furthermore, for those who are able to connect, they may lack the digital savvy required to take advantage of the benefits or protect their rights online.

In this regard, based on the World Summit on the Information Society (WSIS) Forum 2020 discussion, the following priorities have been identified[99]:

- Ensure that no one is left behind in building a digital ecosystem — this includes all ethnicities, races, genders, etc.
- A digital ecosystem should not be seen as a centralised system, but as a way to connect data, promote data standards, identify gaps and stimulate open data and algorithms while protecting privacy.
- Use COVID-19 as an opportunity to move forward — and work to ensure that the digital divide narrows.

Delving deep into the question of "how can digital rights defenders help to create an inclusive future for the internet and digital services in Canada?", action is needed to improve access at every layer — for instance, enhancing digital skills, relevant content, and inclusive workplaces. Literacy is viewed as a key element of capacity building and education in Canada. Resources — either digital or facilitating hardware such as home assistants — can also be developed with marginalised communities in mind to enhance inclusiveness in the digital sphere.

There are increasing concerns around algorithmic bias in digital systems and services. Research has highlighted the impact of developers on the resulting technology, and how technological bias reflects and amplifies existing socio-cultural injustices. Unless marginalised and disadvantaged persons can be involved in developing technologies, those technologies and associated business models will continue to perpetuate inequalities. Further, digital rights defenders can also help to tackle online harassment and demand accountability for online actions. This may include campaigning for improved mechanisms for reporting online abuse and greater accountability of tech platforms through robust legal frameworks. Digital rights defenders may also advocate for anonymity for dissidents and journalistic sources, within accountable, human-rights respecting online spaces. Governments can support digital inclusion through adopting relevant and specific provisions in national digital strategies. Canada could have mechanisms to promote accessibility online as well as issue guidelines regarding public sector procurements. These tools could be used to ensure the adoption of technologies that implement accessibility standards (such as standards on text-to-voice in real-time) or 'universal design' in technical development. Emerging technologies and digital services offer incredible possibilities to create a more inclusive and accessible world. However, unless urgent action is taken to enhance digital inclusion and access, societies will become more polarised, with deepening digital and social divides.

---

[96] Lee Rainie & Jonathan Albright, 'The Future of Free Speech, Trolls, Anonymity and Fake News Online' (Pew Research Centre, 29 March 2017) <https://www.pewresearch.org/internet/2017/03/29/the-future-of-free-speech-trolls-anonymity-and-fake-news-online/> accessed 26 August 2021.

[97] Internet Heath Report 2018, 'How healthy is the internet' <https://internethealthreport.org/2018/> accessed 2 April 2021.

[98] Emily Taylor, 'Bridging the Digital Divide: infrastructure, skills and women's empowerment' (*G20 Insights*, 10 December 2020) <https://www.g20-insights.org/policy_briefs/bridging-digital-divide-infrastructure-skills-womens-empowerment/> accessed 1 April 2021.

[99] WSIS Forum 2020: High-Level Track Outcomes and Executive Brief, <https://www.itu.int/net4/wsis/forum/2020/Files/outcomes/draft/WSISForum2020_HighLevelTrackOutcomesAndExecutiveBrief_DRAFT.pdf> accessed 12 July 2021.

5. How should the digital age of consent be arrived at and what should it be? In pursuance of which child rights should such an age be identified?

The appropriate form of consent (implied or express) depends on a consideration of the sensitivity of the personal information and the reasonable expectations of the individual.[100] Thus, an individual cannot be required to consent to the collection and use of more information than is necessary for the purposes of completing the transaction with the organization. Although *PIPEDA* does not contain a minimum age of consent, the Privacy Commissioner of Canada has suggested that consent of children under 13 years of age would be difficult to obtain. [101] In this regard, a quick comparison with the European Union's *GDPR*[102] could be beneficial in the current scenario, which prescribes a threshold of 16 years of age for digital consent. However, it must be noted here that the individual countries of the EU can lower the age of digital consent varying from 13 to 16 years of age.[103] Although no rule of universal application could be culled out of this comparison, it is important that organizations or online platforms seeking digital consent remain careful while considering whether the individual providing consent has the legal capacity to do so.

Although the internet comes with a multitude of benefits like opportunities for self-expression, access to information, extended scope for interaction and wider horizons of awareness, it has its own drawbacks. It exposes children to a host of threats such as exploitation and abuse by adult users, over-use, cyber-bullying by peers, etc.

There are four foundational rights against which the digital age of consent could ensure to children, which have been stated herein below (accompanied with a brief account). Firstly, all children have a legal right to be safeguarded from abuse, which includes sexual abuse as well. The responsibility lies with state authorities to prevent abusers from contacting children and make the internet a safer place. Secondly, the right to privacy of children is another important right which recognises their sovereignty over their personal information. The corollary of the same would ensure a right to 'be forgotten' — to have data held about oneself erased. Asking children for their consent to collect their information shows respect for children's right to privacy. Consent must be free and informed, and a child must be able to withdraw at any time. If a child does not have the capacity to consent, then their consent can never justify the collection of their information. Further, Canadian courts have interpreted various sections of the Canadian *Charter of Rights and Freedoms*,[104] including the right to life, liberty, and security, and the protection against unreasonable search and seizure, as protecting against unreasonable invasions of privacy. Moreover, the Supreme Court of Canada has recognised the essential role of privacy in a democratic state, stating that "society has come to realize that privacy is at the heart of liberty in a modern state… Grounded in a man's physical and moral autonomy, privacy is essential for the well- being of the individual." [105]

Thirdly, ensuring children's right of access to information and education forms a legal duty of states. The presumption shall be in favour of children's access to the internet, and restrictions shall only be imposed in light of grave factors such as national security, public order or public health. Fourthly, children have a right to freedom of expression and by an extension of that a right to have their views heard in all matters affecting them. Therefore, in pursuance of these above-mentioned rights, a threshold for digital consent would be arrived at.

Public Order

6. How should public order be defined for the digital space? Should situations of disorder in the offline world influence the definition and management of public order online, and if so why and when?

Irrespective of the nature of a polity — democratic or autocratic, federal or unitary — maintenance of public order is universally recognised as the prime function of the state. Anarchy would result if the state failed to

[100] PIPEDA, Schedule 1, cl. 4.3.5.
[101] Timothy Banks, 'GDPR matchup: Canada's Personal Information Protection and Electronic Documents Act' (*IAPP*, 2 May 2017) <https://iapp.org/news/a/matchup-canadas-pipeda-and-the-gdpr/#:~:text=Under%20PIPEDA%2C%20age%20may%20be,is%20no%20strict%20age%20threshold> accessed 18 March 2021.
[102] General Data Protection Regulation 2016.
[103] *Supra* note 20.
[104] Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, *being* Schedule B to the Canada Act, 1982, c. 11 (U.K.), <http://laws-lois.justice.gc.ca/eng/charter/> accessed 29 March 2021.
[105] *R v. Dyment*, [1988] 2 S.C.R. 417.

discharge this duty. Such persistent anarchy would lead to decay and destruction and the eventual disintegration of the state. How then is the public order for the digital space defined?

It is certainly not easy to define the term 'public order' as public morality is relative from a society to another; it is not even the same for individuals inside the same society. This difficulty is heightened by the fact that the internet has no borders between countries, so problems increase in terms of cultural differences where the national public order takes no place. Thus, public order is a flexible concept which depends on the facts, the circumstances, the social context, the values, the fundamental institutions, norms and objectives of the collective, and the needs for stability and public peace. It expresses an axiological content, which represents subjective, changing, and evolutive values.[106]

In light of this, the problems of measuring offline public order will be found more in the digital space. However, the majority of social media has self-regulations which cover any missing issue in national or international legal frameworks. Also, the term is an all-embracing term which invites some ambiguity. However, one thing can be unequivocally stated which is that human rights do apply to online platforms as it has been noted by the United Nations as well.

Further, with regards to the question of "whether the situations of disorder in the offline world influences the definition of public order in digital space", the author opines that the fact is that even if we accept that certain kinds of expression may inspire or incite public disorder, the nexus between the words and subsequent action is far more attenuated on the internet than in any other case. Many kinds of expression which may be provocative in the physical world are far less threatening when appearing on the internet.[107]

Let us now take the famous example of crazed extremists who exchange nerve — gas recipes via the internet. If such instructions are available on an internet news page which is open to an unspecified number of users, this does not necessarily satisfy the conditions of intention to incite a threat to public order. Such recipes may be considered to serve only informative purposes. Nonetheless, downloading such noxious information could be considered an act leading to an offense. In this sense, we should distinguish between the mere possession or consumption of a specific material and the storage, further transmission or use of it. Furthermore, we should distinguish between users who know where to find specific information and users who do not.

7. Should the state be allowed to impose internet shutdowns, slowdowns and communication throttles? What socio-legal rationale could be adopted by states in order to do so?

Rights affected by internet shutdowns, slowdowns, communication throttles: Freedom of expression is a fundamental right enshrined in *Article 19 of the UDHR*[108] and of the *ICCPR*,[109] as well as numerous regional treaties, among them, the *American Convention on Human Rights*, the *African Charter on Human and Peoples' Rights* and *the European Convention on Human Rights*. However, in the past few years, the world has witnessed a massive escalation in censoring practices including internet shutdowns, slowdowns and communication throttles.[110] When the state imposes these restrictions no matter what justifications are advanced, they are interfering with important communication networks. This interference is often characterised as an interference of the freedom of expression.

Internet shutdowns may have the potential to threaten freedom of expression; however, the proposition also involves the sovereign right of states to close telecommunication services. Therefore, the question that arises from this dichotomy is "whether internet shutdown can be justified as an expression of sovereignty of states over their national telecommunication networks?" Contextualizing sovereignty within the framework of internet shutdowns, states should be reasonably afforded a legitimate way to block access to the digital environment as well as suspend digital services coming from other states. For instance, it would be a valid justification for states to shut down digital spaces in light of escalating mass atrocities caused by the dissemination of hate and violent content through social media. The principle of sovereignty entails another

[106] Vimbert, 1993: 701.

[107] Garipis Stylianos, 'Internet and public order' Cyberidentities: Canadian and European Presence in Cyberspace, University of Ottawa Press, Ottawa, 1999, pp. 47–54. JSTOR, <www.jstor.org/stable/j.ctt1cn6rfb.7.> Accessed 3 April 2021.

[108] UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III), <https://www.refworld.org/docid/3ae6b3712c.html>accessed 2 April 2021.

[109] UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, <https://www.refworld.org/docid/3ae6b3aa0.html> accessed 1 April 2021.

[110] Report: the state of internet shutdowns, <https://www.accessnow.org/the-state-of-internet-shutdowns-in-2018/> accessed 12 July, 2021.

expression which is the right to self-defence against the potential use of force. In this context, internet shutdowns would be immensely helpful in avoiding or minimizing the damage caused due to cyber-attacks. It would also protect the state from the external interference of other states.[111]

The doctrine of anticipatory self-defence has been employed within international law for a long time and its credibility has been bolstered both by i) contemporary practice and ii) deductions from the modern weaponry's logic. It is often justified whenever the perceived threat is imminent or there is a necessity that self-defence is instant and overwhelming.

Therefore, in addition to the limitations of the right to freedom of expression, both the principle of sovereignty and the right to self-defence could constitute valid justifications on which the state can rely to limit access to the internet performing practices of internet shutdowns, slowdowns and communication throttles.

Having factored in the argument of internet shutdowns affecting basic tenets of well-recognised human rights, the justifications advanced by states for imposing such restrictions on digital environment have to be assessed through the prism of three principles. The three principles are as follows:

1. Legality: which postulates the existence of law
2. Proportionality: which ensures a rational nexus between the objects and the means adopted to achieve them. It helps in determining whether the legislative measure is disproportionate in its interference with the concerned right.
3. Legitimacy: whether the measure restricting the concerned rights serves a legitimate goal

Social Media Councils

8. Could the Social Media Councils (SMCs) model, as introduced by Article 19, be reinterpreted on a larger scale, with the purpose of monitoring human rights, within the context of Digital Constitutionalism?

A multi-stakeholder approach to online content moderation, as espoused by *Article 19*, through their model of Social Media Councils (SMCs) has substantial advantages for all sides. For platforms, an independent multi-stakeholder body can help to provide legitimacy to their internal processes and demonstrate a commitment to free expression, which is valuable for their public profile. It can also serve as a resource, providing outside perspectives from experts to help navigate particularly complex problems. For governments, these bodies promote the democratic principle of transparency and can help to ameliorate societal concerns about content online. They can also take pressure off courts by creating an accountable body that can moderate many content decisions. For users, the councils will help them better understand the content moderation process and create more transparency about what steps are being taken to protect free speech while addressing issues of abuse.

While some challenging questions about how to develop a successful multi-stakeholder approach to online content moderation remain, there is a convergence on many foundational issues related to content moderation. Further, there is also a consensus on the importance of international human rights law and the protection of free expression as the substantive principles that should guide the work of SMCs. A human rights lens should form the foundation for how we think about all content decisions. Existing human rights standards already provide substantial guidance for how to balance freedom of expression against the risks of certain types of speech (such as inciting violence). These standards provide a universal anchor point for all stakeholders — governments, companies, and users alike.

Their practical usefulness lies in resolving disparities between competing values while remaining relatively sensitive to regional differences. Another advantage that human rights principles provide in addressing challenging issues related to speech online is that, through instruments like *Article 19* of *the International Covenant on Civil and Political Right*s, they provide a clear set of guidelines on what the limits of acceptable speech are and where speech can be reasonably restricted. Even in the case of private companies, while not binding, the UN Guiding Principles on Business and Human Rights provide guidance on how companies should approach their obligations related to human rights.

Additionally, many companies already endorse the human rights framework and apply elements of human rights due diligence in their operations. Working from the premise that a commitment to human rights must

[111] Kilovaty I, "Cyber Operations and International Law. By François Delerue. Cambridge, UK: Cambridge University Press 2020. Pp. Xxii, 513. Index." (2021) 115 American Journal of International Law 187.

underpin any attempts to create new mechanisms for content moderation online does much of the work in ensuring that different stakeholders are on the same page.

C. Privacy, Information Security, and Personal Data

Personal and Non-Personal Data

1. How do we define personal and non-personal data?

The data protection framework in Canada is governed by two laws enforced by the Office of the Privacy Commissioner of Canada:

i. the *Privacy Act*, which covers how the federal government handles personal information[112]

ii. the *Personal Information Protection and Electronic Documents Act (PIPEDA)*, which covers how businesses handle personal information[113]

Section 3 of the Privacy Act[114] defines "personal information" as "information about an identifiable individual that is recorded in any form" and proceeds to provide an inclusive list of illustrations. In addition to what is conventionally regarded as personal information such as biometrics, race, religion, and age, the *Act* protects "views or opinions of another individual about the individual" and "views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual by an institution." *Subsection 2(1) of Part 1 of PIPEDA*[115] defines personal data as "information about an identifiable individual." Additionally, the Canadian provinces of British Columbia, Alberta, and Quebec have their own data protection laws applicable to the private sector which partially displace the federal law in matters pertaining to personal information. However, the definition of personal data remains unchanged under all four statutes as they replicate the same definition stipulated in *PIPEDA*.

There is a reason why the adequacy ruling received by Canada was restricted to commercial organizations: *PIPEDA* only applies to the collection, use or disclosure of personal information in the course of commercial activity. Federally regulated businesses such as banks, airlines, and telecommunications companies also fall under its scope.

What this means is that not-for-profit organizations, such as political parties, associations, educational institutions, and hospitals are outside the jurisdiction of the Canadian data privacy law as long as they do not engage in any commercial activities.[116]

Therefore, although non-personal data is not defined in the Canadian legal framework, There are some instances where *PIPEDA* does not apply. These include:

- Personal information handled by federal government organizations listed under the *Privacy Act*
- Provincial or territorial governments and their agents
- Business contact information such as an employee's name, title, business address, telephone number, or email addresses that is collected, used, or disclosed solely for the purpose of communicating with that person in relation to their employment or profession
- An individual's collection, use, or disclosure of personal information strictly for personal purposes
- An organization's collection, use, or disclosure of personal information solely for a journalistic, artistic, or literary purpose

2. What should be the ethical, economic, and social considerations when regulating non-personal data?

It is difficult to measure the ethical, economic, and social considerations when dealing with non-personal information in a situation where it is not defined in the Canadian legal framework. It is pertinent to note that even though neither the *Privacy Act* nor the *PIPEDA* defines nonpersonal data, there are some instances where *PIPEDA* does not apply. These kinds of data remain unprotected.

---

[112] Privacy Act, 1983 (Cananda).
[113] Personal Information Protection and Electronic Document Act, 2000 (Canada).
[114] Privacy Act, 1983, s3.
[115] Personal Information Protection and Electronic Documents Act 2000, s2(1)..
[116] Andrada Coos, 'Data Protection in Canada' (*Endpoint Protector*, 17 January 2019) < https://www.endpointprotector.com/blog/data-protection-in-canada-pipeda/> last accessed 28th March 2021.

Various research studies show how the susceptibility of anonymised data to the risks of re-identification is extremely high. An experimental study conducted in the US found that data anonymised through the k-anonymity process (one of the techniques mentioned in the report) can be re-identified with a success rate of over 80%. Researchers from the Imperial College, London have further demonstrated that 90% of shoppers were re-identified as unique individuals by using just four random pieces of information.[117] Therefore, a vague standard of anonymization can seriously threaten the privacy of citizens. Moreover, it is possible to collect data from the public assuring them that it is non-personal data and then gaining access to their personal data through de-anonymization.

Another consideration that regulators across the world should take into account is that the sharing of non-personal data does not necessarily lead to a more competitive economy. While some studies have assessed how data can have infrastructural importance in certain markets, they have also acknowledged that such questions are specific to particular domains, firms, and techniques of data processing. Data sharing, therefore, may do little to either curtail economic power or to make firms more competitive.[118]

Scholars in the field of science and technology studies (STS) have warned that we should be wary of thinking about 'data' as a category which is external to and independent of its modes of production, the political economy in which it is produced, or the subject of what is being measured.[119] The implications of this approach could be taking 'data' about communities or society — for example, what they eat or how they move or communicate — collected to serve ads and extract profits from such information — and transposing it in the context of a state function of delivering public benefits, which may be an entirely inappropriate way of observing or calculating what such a community or society requires from the state. Indeed, such data sharing may end up entrenching the power of a few specific firms or systems which create the data.

End-to-end Encryption

3. Should there be a backdoor to end-to-end encryption/Should traceability be enabled to prevent and mitigate instances of online harms? What would the benefits and detriments of the same be?

Encryption is a form of security that prevents outsiders from intercepting information and content as it passes through the web. It secures everything from banking information to military communications to online dating apps.[120] Currently, there is an ongoing debate over so-called 'encryption backdoors', special access points that governments can force or compel tech companies to build. In other words, these are unlocked doors on the web that allow authorities to access encrypted communications without users' consent.[121]

In 1998, Canada adopted its official cryptography policy[122] which rejected the backdoor approaches being pushed at the time. Since then, the government has resisted new calls to weaken encryption, but pressure from allies is growing. Canada's existing legal framework for interception, search, seizure, preservation, and production of data appears to apply to encrypted data or communications.[123] However, there does not appear to be a specific provision in the Criminal Code that imposes requirements on telecommunications providers to decrypt or establishes backdoor access.[124] According to a recent statement by the Royal Canadian Mounted Police (RCMP) quoted in an investigative report by Motherboard, "there is no specific power in the Criminal Code to compel a third party to decrypt or develop decryption tools, nor is there any requirement for

[117] Laura Radelli, 'Unique in the shopping mall: On the reidentifiability of credit card metadata (*Science*, 30 Jan 2015) < https://science.sciencemag.org/content/347/6221/536.full?ijkey=4rZ2eFPUrlLGw&keytype=ref&siteid=sci> last accessed 20th March 2021.

[118] Bundeskartellamt, 'Competition Law and Data' (10 May 2016) https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf;jsessionid=B433476372FD2F7A43EF4F482255113D.1_cid387?__blob=publicationFile&v=2 last accessed 20th March 2021.

[119] Sheila Jasanoff,'Virtual, Visible, and Actionable: Data assemblages and the sightlines of justice' < https://journals.sagepub.com/doi/full/10.1177/2053951717724477> 2053951717724477 last accessed 25th March 2021.

[120] 'What is Data Encryption' (*Forcepoint)* < https://www.forcepoint.com/cyber-edu/data-encryption> last accessed 26th March 2021.

[121] Stuart Thompson, 'Confrontation looming on encryption backdoors as goodale looks for balance' (*National Post*, 7 August 2019) https://nationalpost.com/news/politics/were-closer-to-the-knifes-edge-confrontation-looming-on-encryption-backdoors-as-goodale-looks-for-balance last accessed 5th April 2021.

[122] 'Govrnment Access to Encrypted Communications: Canahttps://fas.org/irp/news/1998/10/981001-crypto.htm

[123] McCarthy Tetrault, *6.0 Cryptography Policies* < http://www.mccarthy.ca/ pubs/cicpaper06.htm> last visited 20th March 2021; Christopher Parsons & Tamir Israel, '*Canada's Quiet History of Weakening Communications Encryption' (The Citizen Lab*, Aug. 11, 2015) < https://citizenlab.org/2015/08/canadas-quiet-history-of-weakening-communications-encryption , *archived at* https://perma.cc/HMT9-B3HW.> last accessed 2nd April 2021.

[124] Government Access to Encrypted Communications: Canada (Library of Congress) <https://www.loc.gov/law/help/encrypted-communications/canada.php> last accessed 7th April 2021.

telecommunications services to provide these services,"[125] but courts may 'compel' third parties like BlackBerry to assist with investigations.[126]

In July 2019, members of the 'Five Eyes' security alliance (the U.S., U.K., New Zealand, Australia, and Canada), are pushing tech companies to build backdoors into their products and services.[127] The countries argue that backdoors are necessary for law enforcement to gain special access to encrypted data during investigations of drug trafficking or organised crime, for example, where other investigative tactics might fall short.[128]

If tech companies are forced to add backdoors for law enforcement, it is likely that bad actors will be right behind them. This would leave popular end-to-end encrypted communications apps such as WhatsApp, Signal, and Telegram vulnerable to exploitation. Backdoors could soon impact billions of users, as the social media giant Facebook plans to expand encryption to its Messenger and Instagram messaging services, despite pushback from governments and overwhelming support from civil society.[129] This is significant, because currently every single unencrypted message is susceptible to privacy abuse, data breaches, malicious hacking, or interception by powerful or malicious actors. Beyond the content of our messages, backdoors can also be used to gain access to interfere with corporate and government communication systems and other infrastructure, undermining public safety.[130] A backdoor to end-to-end encryption can have harmful effects on the functioning of CIRA. Here are some of the major issues introduced by backdoors:

- First, strong encryption is essential to the secure operation of the .CA domain.[131] It helps protect the sensitive, personal information of the owners of over 2.8 million .CA domain names. Encryption also enables several security protocols to prevent phishing attacks, domain hijacking, and other cyberattacks. In fact, the most recent data on cybersecurity shows that 71 per cent of Canadian organizations were victims of such attacks in the last year.[132] Strong encryption ensures that a key component of Canada's internet, which is the servers that keep the .CA domain running, is protected against adversarial state-sponsored actors around the world.[133]

- Second, weakened encryption would have downstream effects for the primary user base: small- to medium-sized businesses across the country.[134] Without reasonable assurance that consumers' financial information is protected from snooping eyes, consumers will lose trust in online commerce, and Canada's digital economy will likely suffer.

- Lastly, at the heart of the encryption debate is the question of trust. It is no secret that public confidence in the internet has taken a tumble. Nearly one-half of Canadians say they have been a victim of a cyberattack according to a survey by the Cybersecure Policy Exchange (CPX) at Ryerson University in Toronto, and it seems that every day there is a new story about Canadians' data being leaked[135]. Right now, Canada needs technologies that help build trust, and strong encryption is one of the best tools for the job.

Regulatory Sandbox

4. How important is compliance with complex/technical/lengthy data protection and privacy statutes in events of crises (e.g. such as during pandemics, where time is essential)? In that regard, is there a need to

---

[125] Jordan Pearson & Justin Ling, '*Exclusive: How Canadian Police Intercept and Read Encrypted BlackBerry Messages*, Motherboard' (Apr. 14, 2016) <http://motherboard.vice.com/read/rcmp-blackberry-project-clemenza-global-encryption-key-canada <https://perma.cc/JK2T-RDQG> last accessed 3rd April 2021.

[126] ibid.

[127] Reuters, 'Security Alliance calls for action' (30 July 2019) https://www.reuters.com/article/us-security-fiveeyes-britain/five-eyes-security-alliance-calls-for-access-to-encrypted-material-idUSKCN1UP199 last accessed 9th April 2021.

[128] ibid.

[129] Joseph Lorenzo Hall, 'Facebook's End to End Encryption Plans' https://cdt.org/insights/open-letter-facebooks-end-to-end-encryption-plans/ last accessed 9th April 2021.

[130] https://www.wired.com/2015/12/researchers-solve-the-juniper-mystery-and-they-say-its-partially-the-nsas-fault/

[131] Bryon Holland, 'Will Canada weaken encryption with backdoors' (*Macleans*, October 2019) <https://www.macleans.ca/opinion/will-canada-weaken-encryption-with-backdoors/> last accessed 3rd April 2021.

[132] CIRCA Cybersecurity Survey, https://www.cira.ca/resources/cybersecurity/report/2019-cira-cybersecurity-survey.

[133] ibid.

[134] Bryon Holland, 'Will Canada weaken encryption with backdoors' (*Maclean's*, 18th October 2019) < https://www.macleans.ca/opinion/will-canada-weaken-encryption-with-backdoors/> last accessed 24th August 2021.

[135] 'More than half of Canadians have been a victim of cyberattacks,' (*CISOMAG*, 13th July 2020) < https://cisomag.eccouncil.org/cyberattacks-on-canadians/> last accessed 25th August, 2021.

provide regulatory sandboxes, and if so what could be the grounding philosophy to shape the rules of control for such ecosystems?

Covid-19 has changed the way we conceive our privacy and the importance we attach to the protection of personal data. Technological tools have been extremely helpful to allow essential activities to continue even when everything else was put to a halt. As the pandemic speeds up digitization, basic privacy principles that would allow us to use public health measures without jeopardizing our rights are, in some cases, best practices rather than requirements under the existing legal framework. [136]

In the Canadian context, risks to privacy and other rights are heightened by the fact that the pandemic is fuelling rapid societal and economic transformations in a context where our laws fail to provide Canadians with effective protection. Privacy acts as a precondition for exercising human rights such as equality rights, in an age when machines and algorithms make decisions about us, and democratic rights, when technologies can thwart democratic processes.

The Office of the Privacy Commissioner of Canada (OPC) has acknowledged that the COVID-19 pandemic requires a flexible and contextual application of privacy laws. It is very important that key principles continue to operate in a democratic country based on the rule of law, even if some of the more detailed requirements are not applied as strictly as they would normally be. The OPC released a framework in April 2020 to assess privacy concerns of initiatives taken in the pandemic. The said framework essentially sets out key principles to be followed in the pandemic without compromising others[137]:

- Legal authority: The proposed measures must have a legal basis.
- Necessity & proportionality: Measures must be necessary and proportionate and therefore be science-based and necessary to achieve a specific identified purpose.
- Purpose limitation: Personal information collected, used, or disclosed to alleviate the public health effects of COVID-19 must not be used for other reasons.
- De-identification measures: De-identified or aggregate data must be used whenever possible.
- Vulnerable populations: Certain information, such as health and precise location data, may have greater sensitivities or disproportionate impacts on vulnerable populations and certain groups of individuals.
- Transparency and accountability: The government should be clear about the basis and the terms applicable to exceptional measures and be accountable for them.
- Time limitation: Privacy invasive measures should be time limited; obligations should end when they are no longer required.

A regulatory sandbox can generally be defined as a controlled environment where for some predetermined period of time and for a defined use case, a close collaboration between firms and a regulator enables firms to test new data uses, technologies, and applications while receiving regulatory guidance.[138] Regulatory sandboxes are especially needed in the financial sector, where regulations have been tightened to protect consumers and investors since the global financial crisis, making it difficult to determine whether to ease these regulations.[139] Moreover, it is not easy to know the effects of new technologies such as financial technology (FinTech) and whether they would have a positive effect on society or not.[140]

In Canada, the Canadian Securities Administrators (CSA) have implemented a regulatory sandbox to create a 'safe space' for FinTech. The process allows organizations to submit innovative business models to the securities regulator and to discuss issues with the applicable securities law, as well as the requirements for compliance.[141]

---

[136] 2019-2020 ANNUAL REPORT TO PARLIAMENT ON THE *PRIVACY ACT* AND *PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT*, HTTPS://WWW.PRIV.GC.CA/EN/OPC-ACTIONS-AND-DECISIONS/AR_INDEX/201920/AR_201920/.

[137] A framework for the government of Canada to assess privacy impactful initiatives (April 2020) https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/fw_covid/ last assessed 9th April 2021.s

[138] Fairchild, R., 'An entrepreneur's choice of venture capitalist or angel-financing: A behavioral game-theoretic approach'. J. Bus. Ventur. 2011, 26, 359–374.

[139] ASIC. ASIC Fintech Regulatory Sandbox; ASIC: Brisbane, Australia, 2019.

[140] Blind, K. The influence of regulations on innovation: A quantitative assessment for OECD countries. Res. Policy 2012, 41, 391–400

[141] Paul Borque, "The CSA as a fintech adopter' https://www.investmentexecutive.com/inside-track_/paul-bourque/thinking-outside-the-box-the-csa-as-a-fintech-adopter/ last assessed 5th April 2021.

Significant factors to shape the rules of such regulatory sandboxes in the Canadian framework[142] are,

1. Is the new solution novel or significantly different from existing offerings?
2. Does the innovation offer an identifiable benefit to customers?
3. Does the business have a genuine need for testing within the sandbox framework?
4. Has the business invested appropriate resources in developing the new solutions, understanding the applicable regulations, and mitigating the risks?
5. Does the business have the intention and ability to deploy the solution in Canada on a broader scale?

Intelligence Agency

5. According to which principles and regulations should intelligence agencies operate online?

Problems arise when privacy is compromised by transnational intelligence gathering. One of the rights at issue in intelligence-gathering activities is information privacy. The right to privacy limits the government's use of personal information, protecting individuals from abuses of government power. Because of the ease with which data can be gathered, stored, and combined in the age of information technology, it is difficult to guarantee its accuracy. At the most basic level, data might be wrongly recorded through human error. When different data sets are combined, information in one of the data sets may be wrongly interpreted because its coding and software systems differ from the other data set's systems. Moreover, the storage capacity of computer systems is so vast that information that has become obsolete, and therefore inaccurate, can be retained indefinitely.[143]

The principles of human dignity and individual autonomy form the basis of the right to privacy.[144] Critical to a liberal society is the individual's power to keep certain matters private and to make other matters public. The duty of others in a liberal society is to respect the individual's decision in favour of privacy. Yet when government agencies collect, combine, and manipulate information on individuals without their consent, they breach that essential duty.

To safeguard privacy interests, most countries have enacted information privacy laws, known in Europe as data protection laws.[145] Such laws specify the conditions under which the government may collect personal information. Generally, individuals must either consent to the collection and the intended uses of their information, or a piece of legislation must specify the public reasons for mandating personal data processing.[146] Furthermore, US privacy law also has a provision that gives individuals the right to apply to government agencies to ensure that information stored in their government files is accurate and that, in every other way, it is being used in accordance with the law.[147]

In the Canadian context, Canada's spy agency recently warned the government that proposed changes to bolster privacy could undermine the ability of intelligence agents to collect and use information about citizens.[148] The OPC oversees compliance with both the *Privacy Act*, governing the federal public sector, and the *Personal Information Protection and Electronic Documents Act*, governing the private sector. Intelligence organizations and operations are subject to the *Privacy Act*, which applies to the personal information practices of federal institutions, to ensure that the privacy of individuals is protected.[149] While the OPC oversees the entire public service for compliance with the *Privacy Act*, specialised bodies were created to handle compliance and review, including privacy, of intelligence operations in Canada: the Security Intelligence Review Committee (SIRC), the Office of the CSE Commissioner (OCSEC), and the Commission for Public Complaints against the RMCP (CPC). Recent events have brought to light new privacy risks within the current political and technological framework of intelligence activities.[150] The evolution of security threats to open,

[142] 'Big Idea; Create regulatory sandboxes' (Canada 2020) https://canada2020.ca/sandbox/.
[143] Francesca Bignami, 'Towards a Right to Privacy in Transnational Intelligence Networks, Michigan Journal of Law.
[144] Stanley I. Benn, Privacy, Freedom, and Respect for Persons, in NoMos XII: PRIVACY 1 (J. Roland Pennock & John W. Chapman eds., 1971).
[145] Privacy Act of 1974, Pub. L. No. 93-579, § 3, 88 Stat. 1897
[146] 5 U.S.C. § 552(e)(3) (2000)
[147] 5 U.S.C. § 552a(d); Convention 108
[148] https://globalnews.ca/news/6954113/csis-privacy-reforms-spy-operations/
[149] *Privacy Act*, R.S.C., 1985, c. P-21, section 2.
[150] Angela Gendron and Martin Rudner, Assessing Cyber Threats to Canadian Infrastructure (March 2012), pp. 21-34.

democratic states — combined with the speed and power of technical surveillance practices and the desire to prevent or prepare for attacks of violence —creates a pressing issue for democratic states to confront.

The Canadian Security Intelligence Service (CSIS) clearly establishes threat definitions and investigatory limits.[151] The *Act* also established the Security Intelligence Review Committee to protect Canadians' rights and freedoms and ensure that CSIS always operates legally and appropriately.[152] Many steps can be taken to prevent intelligence agencies from breaching the online privacy of citizens. These include proactively disclosing annual statistics on cases where they assist other federal agencies with requests for interception, extending existing reporting requirements on use of surveillance, and updating the overview of Canada's intelligence community.

D. Intermediary Regulation

Online Harms and Netizens

1. How do we define online harms?

Online harms are not defined in any particular manner by any legislation or instrument in Canada, but may be considered to include trolling; extortion; bullying and incitement to suicide; child pornography; terrorist activity; propagation of crime;[153] 'industrial-scale' propaganda; and malicious targeting of ethnic, social, or religious minorities. Online harms also include 'doxxing', which refers to the act of "making someone's private information publicly available on the internet."[154]

Rather than laying emphasis on what falls under the definition of online harm, which ends up being more exclusionary than beneficial, there should be a greater emphasis on defining roles of responsibility and jurisdiction, and increasing cooperation among the media, civil society, and the private sector.

2. How should community guidelines for online platforms be drafted, disseminated, and enforced? To what legal standards of accountability and transparency should online platforms be held, and in what capacity? Can you suggest any mechanisms (judicial, or otherwise) which might be capable of ensuring such a check on the functioning of these platforms?

The community guidelines drafting procedure is global and not country-wise; therefore, the community guidelines put in place by several intermediary platforms in Canada do not apply simply to Canada alone. Facebook has semi-monthly global meetings where potential and existing changes to the community standards are discussed, after members of the content policy team have analysed relevant data and carried out extensive research.[155] On Twitter, the development and drafting of a new set of community guidelines or changes in policy are done after in-depth research examining trends in online behaviour. Cultural and social perspectives from different countries are considered, for which the global review teams are trained.[156] A similar process is followed by Google.[157] Presently, most community guidelines are disseminated only when a user makes an account, and later when a policy change is brought about. Community guidelines are enforced by taking down a post after a warning or disabling problematic accounts. Accountability is maintained through the publication of enforcement reports, which provide data according to country.

While drafting community guidelines, users should be given opportunities to be more involved in the process. Community guidelines should be tailored to the countries they are applicable in and must reflect how a certain kind of objectionable behaviour not only violates community guidelines but certain provisions of national law as well. For example, advertising to children must be labelled as objectionable not simply because it contravenes community guidelines, but also because it is prohibited by Canadian law. This becomes even more necessary because Canada's *Bill C-10* requires online platforms to report alleged violators to the

---

[151] Hardy, Timothy S., "Intelligence Reform in the mid-1970s" from CIA Center for the Study of Intelligence Archive, vol. 20, no. 2, pp. 10-13.

[152] Security Intelligence Review Committee, "About SIRC" (October 2012).

[153] 'Community Standard' (*Facebook*) <https://www.facebook.com/communitystandards/introduction> accessed 11 April 2021

[154] 'Internet intermediary liability in Canadian law' (*FRIENDS of Canadian Broadcasting*) <https://friends.ca/workspace/uploads/documents/platform-for-harm-2020-friends.pdf?utm_source=friends&utm_campaign=short-url&utm_medium=organic&utm_content=platformforharm> accessed 11 April 2021

[155] 'Writing Facebook's Rulebook' (*Facebook*, 10 April, 2019) <https://about.fb.com/news/2019/04/insidefeed-community-standards-development-process/> accessed 11 April 2021

[156] 'The Twitter Rules' (*Twitter*) <https://help.twitter.com/en/rules-and-policies/twitter-rules> accessed 11 April 2021

[157] 'Community Guidelines' (*Google*) <https://about.google/community-guidelines/> accessed 11 April 2021

police.[158] With regard to dissemination, it is important to remember that while joining the platform, many people do not read community guidelines and simply agree.[159] It therefore becomes imperative for online platforms to list guidelines in a more engaging manner. This could be done by creating small quizzes on a weekly basis testing user awareness about community guidelines. Short videos explaining the various aspects of online harm and unacceptable behaviour can be prepared and uploaded on the platform, perhaps in an animated video with simple language. Cooperation from local regional teams and dubbing in regional languages by celebrities from different parts of the world will further enhance inclusivity.

The matter of enforcement, however, would require the involvement of active campaigns informing people of the ills of fake bots. Fake news can be fought by providing links to scientifically backed, accurate information. Users should be made aware of how they can be targeted on the basis of religion, political belief, or gender. This would allow online platforms to work in conjunction with users who are more aware of their rights and will therefore demand better enforcement of community guidelines, so that rights may be enjoyed by all.

As a growing number of people begin to rely on online platforms as their main source of news, social media websites must increase the responsibility they assume over content published. Online platforms should be held to the same legal standards as established news houses, which are regulated in Canada by the *Canadian Radio-television and Telecommunications Commission Act*, *Broadcasting Act*, and *Telecommunications Act*.[160] In order to ensure that accountability and transparency are maintained by online platforms, certain measures must be taken.

A six-step program to protect democratic expression online was suggested by the Canadian Commission on Democratic Expression. This includes the imposition of duties on platforms to act responsibly, the need for a new regulatory body, the formation of a social media council, transparency measures, remedies for individual content harms, and quick takedown measures.[161]

In the past, the Canadian government has been committed to protecting online democratic expression. During the 2019 elections, a Protecting Democracy strategy was taken up by the government, spreading awareness about online threats to democracy through the Digital Citizen initiative.[162] This allowed the 2019 elections to run smoothly. Further, the Canadian Parliament has taken a three-pronged approach towards tackling the accountability of online platforms in Canada by introducing *Bill C-36*, *Bill C-10*, and additional legislation for the media.[163] *Bill C-36* was introduced with the aim to tackle online hate by amending Canada's *Criminal Code* and *Canadian Human Rights Act*. Under *Bill C-36*, the *Canadian Human Rights Act* will be amended to make the communication of hate speech through the internet and online platforms a "discriminatory practice". If a person fears that another will commit an offence which is "motivated by bias, prejudice or hate based on race, national or ethnic origin, language, colour, religion, sex, age, mental or physical disability, sexual orientation, gender identity or expression, or any other similar factor," the person is permitted, with the consent of the Attorney General, to appear before a provincial court. This *Bill* defines 'hate' as "the emotion that involves detestation or vilification and that is stronger than dislike or disdain." Through *Bill C-36*, victims of online hate speech will be allowed to file a formal complaint with the Canadian Human Rights Commission.[164]

Bill C-10, on the other hand, proposes several amendments to the Broadcasting Act, in order to empower the CRTC to regulate Canadian and foreign online platforms and impose monetary penalties on broadcasting companies. This *Bill* also seeks to bring about greater discoverability of Canadian content, so that Indigenous

---

[158] Dwayne Winseck, 'Bill C-10 and the Future of Internet Regulation in Canada' (*Centre for International Governance Innovation*, 2 June 2021) <https://www.cigionline.org/articles/bill-c-10-and-the-future-of-internet-regulation-in-canada/> accessed 28 August 2021

[159] David Berreby, 'Click to agree with what? No one reads terms of service, studies confirm' (*The Guardian*, 3 March 2017) <https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print> accessed 11 April 2021

[160] 'Canadian Radio-television and Telecommunications Commission: Statutes and Regulations' (*Government of Canada*) <https://crtc.gc.ca/eng/statutes-lois.htm> accessed 11 April 2021

[161] 'Harms Reduction: A Six-Step Program to Protect Democratic Expression Online' (*Public Policy Forum*) <https://ppforum.ca/articles/harms-reduction-a-six-step-program-to-protect-democratic-expression-online/> accessed 11 April 2021

[162] 'Online Disinformation' (*Government of Canada*) <https://www.canada.ca/en/canadian-heritage/services/online-disinformation.html> accessed 11 April 2021

[163] Janet E. Silver, 'Regulation of online hate speech coming soon, says minister' (*iPolitics*, 29 January 2021) <https://ipolitics.ca/2021/01/29/regulation-of-online-hate-speech-coming-soon-says-minister/> accessed 11 April 2021

[164] Eric Stober, 'Liberals introduce bill to fight online hate with Criminal Code amendments' (*Global News*, 23 June 2021) <https://globalnews.ca/news/7976076/bill-c-36-online-hate-canada/> accessed 28 August 2021

cultural diversity is adequately represented in media.[165] However, it has drawn flak for several reasons, like inconsistencies in statements regarding its contents, reduction in consumer choice, ambiguity in the wording of the *Bill*,[166] provisions for 24-hour notice and takedown, excessive power granted to the CRTC, and potential clampdowns on freedom of speech and expression. While discussions are taking place with respect to regulation, Canadian judges have been making attempts to halt online harms and trolling, especially in cases of defamation, by making larger damage awards and more robust injunctive orders.[167]

Therefore, online platforms are being held to high legal standards of accountability despite falling under the capacity of intermediaries. Several mechanisms, as explained above, are being implemented to ensure a check on the functioning of online platforms.

3. Should online platforms be immune from liability from third-party, user generated content [refer to intermediary liability laws]?

This liability must extend to user-generated content as well. In recent years, online platforms have been responsible for the spread of terrorism-related activity.[168]

This raises the question regarding whether such liability can legally be imposed upon online platforms. While the United States-Mexico-Canada Agreement provides protection to intermediaries, it must be noted that companies have basic obligations to society which are not being upheld when they allow offensive and illegal content (which often violates international human rights) to proliferate, and therefore intermediaries should not be indemnified from the same. It is this obligation that provides Canadian legislatures a caveat allowing them to enact and pursue domestic legislation to reduce the broad indemnity enjoyed by online intermediary platforms.[169] This includes *Bill C-36* and *Bill C-10*. However, although these measures are a step forward towards intermediary liability, they come with their own set of flaws, which have been discussed above.

The balance between freedom of speech and expression with other rights can be achieved through government regulation. Further, in considering the liability of intermediaries, the 'needle in a haystack' defence often provided by online platforms must be ignored. Platforms have admitted to being in possession of advanced tools and technologies which they use to understand the content of their users' posts and needs while appealing to advertisers. However, when dealing with regulators, they present themselves as though they possess no means to regulate user-generated content. To prevent the clogging of courts by rising litigation, a specialised tribunal may be set up to mediate disputes between users and internet platforms. Meaningful and proportionate sanctions must be applied.

Therefore, online platforms should not be immune from liability from third-party, user generated content, and the above recommendations must be effectively implemented to reduce the incidents and impact of online harms.

4. What should the parameters to define problematic user-generated content be?

Problematic user-generated content should be seen as synonymous to online harms. To this end, several intermediaries have defined unacceptable behaviour in their community guidelines, which are applicable not only to Canada but globally. The community standards of Facebook lay down what is unacceptable, and their parameters include violence and criminal behaviour, security, offensive content, violation of integrity and authenticity, and violation of intellectual property rights. Violence and criminal behaviour comprise helping harm and promoting crime, cheating and manipulation, and dealing with regulated goods like drugs. Security

[165] Scott Prescott, 'Canada: Bill C-10: Regulating Online Streaming Services – The Canadian Model' (*Mondaq*, 30 June 2021) <https://www.mondaq.com/canada/social-media/1086012/bill-c-10-regulating-online-streaming-services-the-canadian-model> accessed 28 August 2021

[166] Michael Geist, 'The Broadcasting Act Blunder, Day 20: The Case Against Bill C-10' (*Michael Geist*, 18 December 2020) <https://www.michaelgeist.ca/2020/12/the-case-against-bill-c-10/> accessed 28 August 2021

[167] Mark A.B. Donald, 'Bringing order from chaos: some thoughts on recent judicial approaches to online libel cases' (2019) 1 (3) The Advocates' Journal <https://www.scribd.com/document/439971183/Bringing-Order-from-Chaos-Mark-Donald-TheAdvocates-Journal-Winter-2019> accessed 11 April 2021

[168] Jennie Marsh, Tara Mulholland, 'How the Christchurch terrorist attack was made for social media' (*CNN*, 16 March 2019) <https://www.cnn. com/2019/03/15/tech/christchurch-internet-radicalization-intl/index.html> accessed 11 April 2021

[169] Michael Geist, 'Eric Goldman on Internet Platform Liability and the Trump Executive Order' (Michael Geist, 8 June 2020) <https://www.michaelgeist.ca/podcast/episode-54-eric-goldman-on-internet-platform-liability-and-the-trump-executive-order/> accessed 11 April 2021

refers to content that displays suicide or self-harm, sexual abuse and nudity of children, sexual and human exploitation of adults, bullying and harassment, and privacy violations. Offensive content refers to hate speech, violent and offensive content, adult nudity and sexual activity, sexual urges, ruthlessness, and insensitivity. Adult nudity is allowed in cases of art, protests, and images of breastfeeding. Violations of integrity and authenticity include spam, fake news, and account authenticity. Violations of intellectual property rights include trademarks and copyrights and other legal rights which are not allowed to be infringed upon.[170] Similar guidelines were laid down by Twitter[171] and Google.[172]

The parameters laid down in the community guidelines are reasonable and just in nature. However, user-generated content should not be deemed problematic simply because it contradicts political opinions or provides criticism in a factually accurate manner. In defining problematic user-generated content, the parameters must never be arbitrary and must uphold principles of natural justice and should be in line with domestic laws as well as international treaty obligations and human rights.

5. Should online platforms moderate 'fake news', and if so, why?

The increase in the spread of fake news as a result of the growth of online platforms has necessitated demands for regulation, because fake news is often divisive, can instigate prejudice, and can pose threats to democracy itself. Many argue that Canada is better off with respect to fake news and misinformation compared to other countries.[173] This includes fake news in the online sphere as well. During the 2019 elections, special care was taken to minimize the role of fake news. This was done by introducing transparency guidelines for political advertising online, setting up a cybersecurity task force, allocating $7 million Canadian dollars towards awareness campaigns, and establishing a non-partisan panel which had the power to bring potential events of foreign interference in the election to the notice of the public.[174]

It is necessary for online platforms to take responsibility for fake news that is proliferated through the medium of their websites and applications. This is because, even though they are mere intermediaries, they provide a platform for fake news to be spread on a faster level than ever before. As a growing number of people begin to rely on online platforms as their main source of news and information, especially during a pandemic, it becomes imperative for social media websites to increase the responsibility they assume over the content published. Twitter Moments, a feature displaying brief snapshots of the daily news, is the best example to support this.[175] Additionally, one-third of Canadians have been reported to be relying on social media as a primary source of financial information.[176] Currently, social media companies must either prevent false news outright, as was done by Pinterest with regard to anti-vaccination, or provide verified and vetted information that would debunk the misguided claims made in fake or hateful content.[177]

However, fake news and misinformation cannot be regulated by online platforms alone. Community guidelines of these online platforms are universal in nature, and implementational challenges must be ameliorated by the government complementing the regulation task undertaken by online platforms. This legislative support may be minimal and limited in nature but is necessary to bring about a more efficient and effective regulatory mechanism.[178] Therefore, it is required for online platforms to moderate fake news in cooperation and harmony with governments, through adequate and rational legislation.

---

[170] 'Community Standard' (*Facebook*) <https://www.facebook.com/communitystandards/introduction> accessed 11 April 2021

[171] 'The Twitter Rules' (*Twitter*) <https://help.twitter.com/en/rules-and-policies/twitter-rules> accessed 11 April 2021

[172] 'Community Guidelines' (*Google*) <https://about.google/community-guidelines/> accessed 11 April 2021

[173] 'Lessons in Resilience: Canada's Digital Media Ecosystem and the 2019 Election' (*Public Policy Forum*) <https://ppforum.ca/wp-content/uploads/2020/05/DDP-LessonsInResilience-MAY2020-EN.pdf> accessed 11 April 2021

[174] Alexandra Samuel, 'To Predict the Role of Fake News in 2020, Look to Canada' (*JSTOR Daily*, 15 October 2019) <https://daily.jstor.org/to-predict-the-role-of-fake-news-in-2020-look-to-canada/> accessed 28 August 2021

[175] 'Explore' (*Twitter*) <https://twitter.com/explore> accessed 11 April 2021

[176] 'One-third of Canadians relying on social media or friends as primary source of financial information' (*Business Wire*, 8 June 2021) <https://www.businesswire.com/news/home/20210608005381/en/One-third-of-Canadians-relying-on-social-media-or-friends-as-primary-source-of-financial-information> accessed 28 August 2021

[177] Niam Yaraghi, 'How should social media platforms combat misinformation and hate speech?' (*Brookings*) <https://www.brookings.edu/blog/techtank/2019/04/09/how-should-social-media-platforms-combat-misinformation-and-hate-speech/> accessed 11 April 2021

[178] 'ARTICLE 19's response to recognition of IMPRESS' (*Article 19*) <https://www.article19.org/resources/article-19s-response-to-recognition-of-impress/> accessed 11 April 2021

6. Should safe-harbour protections be offered to online platforms, given that the grant of such a protection will come at the cost of fundamental rights (e.g. privacy) of citizens? If affirmative, how should this balance be achieved? [Read with Questions in Part B.]

A 'safe harbour' refers to immunity that is provided to intermediaries for protection from any form of liability for the unlawful acts of third parties, unless the platform had prior knowledge that illegal content was stored on, or illegal actions were being committed though their platform.[179]

As the role of online platforms shifts from a neutral and passive intermediary to a major source of news and other information, it is important to question the principle of safe harbour for intermediaries. The United States-Mexico-Canada Agreement, by providing protection to intermediaries, was initially praised for upholding citizens' rights to freedom of speech and expression.[180]

However, with a recent increase in online harms, the benefits of providing a safe harbour to online intermediary platforms no longer seem to outweigh the negatives. It must be noted that companies have basic obligations to society which are not being upheld when they online harms are allowed to proliferate through their platforms. With respect to online harms pertaining to copyright infringement through online platforms, the launch of a public consultation on Canada's copyright framework for online intermediaries was announced in April 2021. This sought to address issues like safe harbour protections for intermediaries, remuneration for the online use of copyright-protected content, and the enforcement tools available to combat online infringement.[181]

Globally, solutions to this question have been found through examples like Germany's *Netzwerkdurchsetzungsgesetz* (an Act to Improve the Enforcement of the Law in Social Networks). The German *Netzwerkdurchsetzungsgesetz*, describes 'high-risk' to include child-harming content; and material that incites violence, religious intolerance, or enmity. Such content is banned or removed expeditiously within 12–24 hours. Content that is not 'manifestly' unlawful, like copyright violations, can be deleted in a longer timeframe, within seven days.[182] This appears to be a better alternative to the Canadian *Bill C-10*, which has only 24-hour notice and takedown, which may prove detrimental due to bias on the basis of prejudice and stereotypes on the part of human moderators.[183] On the other hand, better self-regulation by intermediaries can be done by online platforms coming together and designing a format that users can utilise to report illegal content, a compilation of which can be used to analyse trends pertaining to the removal of content and user behaviour.

Therefore, safe-harbour protections should not be offered to online platforms, and a balance has to be sought between extreme regulation by the government and self-regulation. Such a balance must be sought by rational means and application of judgement. Indeed, inaction on the part of intermediaries will no longer be an option and steps must be taken collectively by governments, online platforms, and users to find workable solutions.

Regulating Online Intermediaries

7. How does the global intermediary ecosystem shift from a post-hoc, harm-prevention lens to a proactive approach towards understanding and regulating technology?

Currently, the perspective that has been appropriated by the global intermediary ecosystem heavily emphasises a harm prevention approach. In light of the COVID-19 pandemic, where fake news and online harms have had particularly dire ramifications, such a perspective was crucial, as online platforms allowed the

[179] Tanya Dayal, 'India: Intermediary Liability: Evolution Of Safe-Harbour Law In India (Part I)' (*Mondaq*, 2 January 2020) <https://www.mondaq.com/india/it-and-internet/879480/intermediary-liability-evolution-of-safe-harbour-law-in-india-part-i> accessed 11 April 2021

[180] Michael Geist, 'Why the USMCA will enhance online free speech in Canada' (*Policy Options*, 4 October 2018) <https://policyoptions.irpp.org/magazines/october-2018/why-the-usmca-will-enhance-online-free-speech-in-canada/> accessed 28 August 2021

[181] Casey Chisick, Lauren White and Jessica Zagar, 'Government of Canada launches consultation on a modern copyright framework for online intermediaries' (*Cassels*, 15 April 2021) <https://cassels.com/insights/government-of-canada-launches-consultation-on-a-modern-copyright-framework-for-online-intermediaries/> accessed 28 August 2021

[182] 'Network Enforcement Act (Netzdurchsetzunggesetz, NetzDG)' (German Law Archive) <https://germanlawarchive.iuscomp.org/?p=1245> accessed 11 April 2021

[183] Tracy Jan and Elizabeth Dwoskin, 'A white man called her kids the n-word. Facebook stopped her from sharing it' (*Washington Post*, 31 July 2017) <https://www.washingtonpost.com/business/economy/for-facebook-erasing-hate-speech-proves-a-daunting-challenge/2017/07/31/922d9bc6-6e3b-11e7-9c15-177740635e83_story.html?noredirect=on&utm_term=.79e540401fa9> accessed 28 August 2021

proliferation of medical misinformation, false advertising of products that claimed to cure coronavirus, and xenophobia against Asians.

As a result, globally, intermediaries and governments have relied upon a harm-prevention perspective. Canada in particular has taken online harm seriously, with *Bill C-36* being introduced with the aim to tackle online hate by amending Canada's *Criminal Code* and *Canadian Human Rights Act*, and *Bill C-10* recently passed to modify the *Broadcasting Act*.[184]

However, moving forward, there should be a shift towards a more in-depth analysis of technology, not just to prevent rights from being infringed, but in order to understand how technology can be better used and regulated to ensure that the rights already guaranteed to people are enjoyed by all. This would involve finding solutions to increase freedom of speech and expression of repressed communities by providing greater access to technology. Research reveals how access to internet and mobile phones is gendered,[185] a disparity that is deepened by racial differences.[186] This disallows women from participating and expressing their opinions on online platforms.

A proactive approach would also mean reworking the algorithm, albeit in a manner that does not push one agenda or one point of view alone. A holistic approach must be taken while presenting data, by displaying different opinions instead of pushing one viewpoint through the algorithm, and such a measure may allow the user to make an informed decision independently.

8. Do the guidelines/policies of online platforms account for fallibility of the algorithm and the human content moderators, and if so, to what extent?

Algorithms are often susceptible to manipulation by bots, and the job of human content moderators becomes increasingly impossible due to the rising number of users in the digital sphere. Recently, questions have been raised regarding algorithm regulation by the CRTC under *Bill C-10*. This was denied by Canadian Heritage Minister Steven Guilbeault, but a considerable amount of ambiguity was created when he stated in Parliament that *Bill C-10* would bring about a greater discoverability and visibility of Canadian content on online platforms. It remains to be seen how far the CRTC can regulate algorithms under in Canada.[187]

Globally, Facebook uses its algorithms to 'down rank' content in the news feed that is not proved to be accurate or authentic. In important situations, such as elections, Facebook has hired human fact-checkers to flag false content, which will consequently be demoted in users' news feeds.[188] Google has been working on introducing a 'fact check label' which flags a claim that has been fact-checked by a publisher or fact-checker, and links the claim to the source. On YouTube, the algorithms have been improved upon so that authoritative sources of news are prioritised over clickbait.[189] Measures were also taken by Twitter to actively develop technology to prohibit malicious bots. [190] However, demotion of false content is not sufficient as false content may continue to spread public alarm, as revealed during the Las Vegas shooting in October 2017.[191]

Consequently, it becomes necessary for social media companies to use a combination of partnering, AI, crowdsourced misinformation detection, human fact-checkers, and collaborating with news organizations, as none of these methods alone will be successful.

---

[184] Janet E. Silver, 'Regulation of online hate speech coming soon, says minister' (*iPolitics*, 29 January 2021) <https://ipolitics.ca/2021/01/29/regulation-of-online-hate-speech-coming-soon-says-minister/> accessed 11 April 2021

[185] 'Bridging the gender divide' (*ITU*) <https://www.itu.int/en/mediacentre/backgrounders/Pages/bridging-the-gender-divide.aspx#:~:text=Challenges%20and%20solutions-,A%20substantial%20divide%20persists%20between%20women%20and%20men%20and%20between,gap%20is%2017%20per%20cent> accessed 11 April 2021

[186] Sarbani Banerjee and Amitra Hodge, 'Internet Usage: A Within Race Analysis' (2007) 14 (3) Race, Gender & Class Journal <https://www.jstor.org/stable/41675301?seq=1> accessed 11 April 2021

[187] Rachel Gilmore, 'Could Bill C-10 regulate your social media algorithm? Minister responsible won't say' (*Global News*, 14 May 2021) <https://globalnews.ca/news/7862794/bill-c-10-social-media-free-speech-broadcasting-act/> accessed 28 August 2021

[188] 'Community Standards Enforcement Report, November 2019 Edition' (*Facebook*) <https://about.fb.com/news/2019/11/community-standards-enforcement-report-nov-2019/> accessed 21 March 2021

[189] Barry Schwartz, 'Google Brain Canada: Google Search Uses Click Data for Rankings?' (*Search Engine Round Table*, 11 September 2017) <https://www.seroundtable.com/google-brain-click-data-for-rankings-24441.html> accessed 11 April 2021

[190] Chris Fox, 'Twitter: Algorithms were not always impartial' (*BBC*, 6 September 2018) <https://www.bbc.com/news/technology-45426407> accessed 11 April 2021

[191] Richard Waters, 'Facebook and Google help showcase Las Vegas fake news' (*Financial Times*, 3 October 2017) <https://www.ft.com/content/030184c2-a7f1-11e7-ab55-27219df83c97> accessed 11 April 2021

9. What role should community guidelines drafted by online platforms play in the governance of user-generated content? How should the terrain of conflict between community guidelines, public policy domestic contexts, and international human rights be negotiated upon?

With regard to Google and YouTube, the same community guidelines are in place all over the world. Since it operates in more than 100 different countries, each country has unique problems and, from time to time, something may be posted on the Google platform that is objectionable in nature, not fully complying with either the community guidelines or the laws of the country. Therefore, Google has put into place various processes to review and act on valid legal requests based on local laws, wherever applicable.

Community guidelines have a crucial role to play in the governance of user-generated content. The terrain of conflict between community guidelines, public policy domestic contexts, and international human rights must be negotiated upon by improving the implementation of community guidelines. Due to a lack of real accountability of online platforms, the time taken to remedy the situation can often be very long. Some ways of remedying this are the aforementioned examples of Germany's *Netzwerkdurchsetzungsgesetz* and the six-step program of the Canadian Commission on Democratic Expression. The latter includes the imposition of duties on platforms to act responsibly, the need for a new regulatory body, the formation of a social media council, transparency measures, remedies for individual content harms, and quick takedown measures.[192]

Political Advertising

10. Should the advertisement policies and sponsored content of online platforms adhere to certain standards (e.g. of whether they interfere with the political opinions and elections in a democracy)? If so, who should frame these policies, and who should be the final arbiter?

Advertisements can often be misused by being intentionally deceptive, denying the customer the right to make an informed decision. Advertisements online are more sensitive since they are more widely accessible. Children in particular can be more susceptible to the influence of advertisements. In Quebec, advertising to children is prohibited; children are defined as those aged under 13. This is dealt with in Office de la protection du consommateur; Broadcast Code for Advertising to Children published by the Canadian Association of Broadcasters in cooperation with Advertising Standards Canada and the Canadian Code of Advertising Standards.[193] During elections, advertisements can influence the opinions of the majority regarding divisive topics. During the 2019 Canadian election, there was a total ban on political advertisements. This was followed by Facebook, Twitter and Google.[194] Moreover, it is important to ensure the accuracy of goods and services being advertised. Health Canada has implemented new guidelines regarding regulated substances associated with the Covid-19 pandemic.[195] Targeted advertising remains a major problem. According to a study carried out by network theorists, when misinformation is targeted towards those who are predisposed to believe this fake news, it spreads further.[196]

Therefore, advertisement policies of online platforms must adhere to certain standards. There should be country specific teams in companies to look into a country's specific needs. The final arbiter should be an independent third-party committee comprising people from the judiciary, executive, and legislature, along with representatives from the online platform itself.

[192] 'Harms Reduction: A Six-Step Program to Protect Democratic Expression Online' (*Public Policy Forum*) <https://ppforum.ca/articles/harms-reduction-a-six-step-program-to-protect-democratic-expression-online/> accessed 11 April 2021

[193] 'Advertising to Canadians' (*Osler*) <https://www.osler.com/en/resources/business-in-canada/browse-topics/selling/advertising-to-canadians> accessed 11 April 2021

[194] Bill Curry, 'Elections Canada puts Facebook, Google, other tech giants on notice over political ads' (*The Globe and Mail*, 24 April 2019) <https://www.theglobeandmail.com/politics/article-elections-canada-puts-tech-giants-on-notice-over-political-ads/> accessed 11 April 2021

[195] 'Health Canada Issues Guidelines on Covid-19 Regulated Substances' (*IAB Canada*) <http://iabcanada.com/iab-standards-and-guidelines/health-canada-issues-guidelines-on-covid-19-regulated-substances/> accessed 11 April 2021

[196] 'Report of the Select Committee on Deliberate Online Falsehoods – Causes, Consequences and Countermeasures' (*Parliament of Singapore*) <https://sprs.parl.gov.sg/selectcommittee/selectcommittee/download?id=1&type=subReport> accessed 11 April 2021

Conclusion

When you are online, online privacy, sometimes called internet privacy or digital privacy, relates to how much of your personal, financial, and browsing information is kept secret. This has been an increasing concern, as browser history and personal information are all at danger when using the internet. Many people overlook the importance of internet privacy, but they should be conscious of how much information they're disclosing — not just on social media, but even when they're just browsing. It is vital to keep in mind that nothing is free, whether it is installing applications, utilising a company's 'free' email service (like Gmail), or accessing social media sites like Facebook. Even accessing a website entails sharing personal information. And, just as some people in your life are more familiar with you than others, online privacy is a spectrum: certain platforms collect and store more information about you than others.

Because regulations governing how digital companies collect data about their users are obsolete or non-existent, the largest platforms all require consumers to opt-out of having their data gathered rather than allowing them to opt-in. This means that the power is in the hands of the firms, not the users, by default. The extent of the data on the user that is being stored is frequently not disclosed to the user. This is why a research study on various aspects of digital freedoms is imperative to understand what all steps are required to ensure that the right to privacy of every citizen is protected.

When it comes to Digital Constitution, China's approach is laudable and it has, in fact, become an example for others to follow. However, to harmonize diverse national frameworks in order to achieve a global digital Constitution, a multijurisdictional approach is required which involves establishing a common definition of digital economy and a list of key indicators for monitoring developments related to growth in digital economy.

On similar lines to its *Charter of Rights and Freedoms*, Canada's *Digital Charter* provides foundational principles for its future policy framework surrounding digital sphere. It plays an important role in defining digital Constitutionalism and its core tenets in Canada. A constitutional model for technological changes will need to address diversity of content, regulation of social media platforms. It should consider and if needed, amend the legislative framework on privacy, competition law, evidentiary standards and cyber security. The role of grassroot, judicial and social media actors will be relevant here. Further, cross-border nature of digital transactions demands national frameworks to multi-jurisdictional privacy and data protection regulations.

Moreover, answering the question of "How can digital rights advocates contribute to a more equitable internet and digital services future in Canada?", it is concluded that action is needed at every level to improve access, such as improving digital skills, appropriate content, and inclusive workplaces. With regards to the question of digital age of consent, it is found that online platforms seeking digital permission exercise caution when determining whether the person providing consent has the legal capacity to do so. Four fundamental rights have been identified in this regard which are as follows:

i) Legal right to be safeguarded from abuse
ii) Right to privacy of children
iii) Right of access to information and education forms
iv) Right to freedom of expression

Furthermore, it is opined that it is difficult to define public order since it is a fluid term that is influenced by specific facts, circumstances and the social context, etc. In this regard, it is concluded that while there are considerable socio-legal reasons for the states for imposing restrictions on the use of internet, any sort of restriction must meet the test of legality, proportionality and legitimacy. Lastly, a multi-stakeholder approach as envisioned by *Article 19* through Social Media Councils is deliberated upon in the context of digital Constitutionalism. Resultantly, it is found that SMCs have substantial advantages for all sides.

When it comes to the aspect of Information Privacy, it is important that Canada builds a strong encryption mechanism for the protection of both personal and non-personal data. Further, a contextual and flexible application of privacy laws is needed in times of crises. It is crucial that the fundamental rights of the citizens are protection even if it means compromising with the strict application of the privacy statutes. Some of the key principles that should be taken into account by authorities in times of crises are; Legal Authority, Necessity and Proportionality, Purpose Limitation, Transparency, Accountability etc.

ANNEXURE

Questionnaire | Project Aristotle

a. Digital Constitutionalism and Internet Governance

1. What factors can be considered important to ground Digital Constitutionalism in traditional Constitutional concepts?
2. How can we define Digital Constitutionalism?
3. What should be the core tenets of a Digital Constitution?
4. How can Digital Constitutionalism present a Constitutional model for the people, by the people, and of the people?
5. How can online platforms be made more inclusive, representative, and equal?
6. What role should open-source intelligence (=OSINT: the discipline of assembling and analyzing publicly available information) play in the future of our society?
7. Should the Digital Constitution be an integrative model, which draws upon and comprehensively presents standards for specific laws (e.g. antitrust, evidentiary standards etc.) as opposed to grounding ideals? If so, how should it fulfil the responsibilities of a pluralistic enterprise such as this as well as the specific needs of a pluralistic global society?
8. How can competition and antitrust laws of different jurisdictions protect the global market from big-tech domination, and is there a need to?
9. What is the role of regional/grassroots actors as well as inter-judicial cooperation/coordination in the digital ecosystem? Which other mechanism(s) might be more helpful?
10. Can the Digital Constitution present an anchor for the governance of the virtual world similar to a traditional Constitutional model or will it always be in flux? Is there a need for Constitutional innovation, and if so, in which areas (e.g. the right to be forgotten as a novel right)?
11. How is it possible to harmonise diverse national frameworks in order to achieve a global Digital Constitution?

b. Human and Constitutionally Guaranteed Rights:

1. Which human and Constitutionally guaranteed rights do online platforms affect, and how?
2. Who can be defined as a netizen?
3. Who can be classified as a 'bad actor', and can 'bad actors' be netizens?
4. How can we embed within the digital ecosystem approaches which are responsive to the needs of minorities (e.g. ethnic minorities, racial minorities, gender minorities, religious minorities)?
5. How should the digital age of consent be arrived at and what should it be? In pursuance of which child rights should such an age be identified?
6. How should public order be defined for the digital space? Should situations of disorder in the offline world influence the definition and management of public order online, and if so why and when?
7. Should the state be allowed to impose internet shutdowns, slowdowns and communication throttles? What socio-legal rationale could be adopted by states in order to do so?
8. Could the Social Media Councils (SMCs) model, as introduced by Article 19, be reinterpreted on a larger scale, with the purpose of monitoring human rights, within the context of Digital Constitutionalism?

c. Privacy, Information Security, and Personal Data:

1. How do we define personal and non-personal data?
2. What should be the ethical, economic, and social considerations when regulating non-personal data?
3. Should there be a backdoor to end-to-end encryption/Should traceability be enabled to prevent and mitigate instances of online harms? What would the benefits and detriments of the same be?
4. How important is compliance with complex/technical/lengthy data protection and privacy statutes in events of crises (e.g. such as during pandemics, where time is essential)? In that regard, is there a need to provide regulatory sandboxes, and if so what could be the grounding philosophy to shape the rules of control for such ecosystems?

5. According to which principles and regulations should intelligence agencies operate online?

d. Intermediary Regulation:

1. How do we define online harms?
2. How should community guidelines for online platforms be drafted, disseminated, and enforced? To what legal standards of accountability and transparency should online platforms be held, and in what capacity? Can you suggest any mechanisms (judicial, or otherwise) which might be capable of ensuring such a check on the functioning of these platforms?
3. Should online platforms be immune from liability from third-party, user generated content [refer to intermediary liability laws]?
4. What should the parameters to define problematic user-generated content be?
5. Should online platforms moderate 'fake news', and if so, why?
6. Should safe-harbour protections be offered to online platforms, given that the grant of such a protection will come at the cost of fundamental rights (e.g. privacy) of citizens? If affirmative, how should this balance be achieved? [Read with Questions in Part B.]
7. How does the global intermediary ecosystem shift from a post-hoc, harm-prevention lens to a proactive approach towards understanding and regulating technology?
8. Do the guidelines/policies of online platforms account for fallibility of the algorithm and the human content moderators, and if so, to what extent?
9. What role should community guidelines drafted by online platforms play in the governance of user-generated content? How should the terrain of conflict between community guidelines, public policy domestic contexts, and international human rights be negotiated upon?
10. Should the advertisement policies and sponsored content of online platforms adhere to certain standards (e.g. of whether they interfere with the political opinions and elections in a democracy)? If so, who should frame these policies, and who should be the final arbiter?

Institute
for Internet &
the Just Society