Research Program
on Digital Constitutionalism
Project Aristotle

New Zealand

Country Report

December 2021

Authors

A Janhavi, NLSIU Legal Services Clinic
Aditi Sheth, NLSIU Legal Services Clinic
Anushya, NLSIU Legal Services Clinic
Pratyush Singh, NLSIU Legal Services Clinic
Shriya, NLSIU Legal Services Clinic

Institute
for Internet &
the Just Society

project
Aristotle

Research Program on Digital Constitutionalism **Project Aristotle**

New Zealand

Country Report

Authors
A Janhavi, NLSIU Legal Services Clinic
Aditi Sheth, NLSIU Legal Services Clinic
Anushya, NLSIU Legal Services Clinic
Pratyush Singh, NLSIU Legal Services Clinic
Shriya, NLSIU Legal Services Clinic

December 2021

Inquiries may be directed to digitalgovdem@internetjustsociety.org

DOI: 10.5281/zenodo.5792087

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

New Zealand has established itself as a major presence in the digital space. It has taken multiple initiatives to carry its work online and ensure that its citizens benefit from it. The government has been playing a very active role in institutionalizing digital governance as well as bringing about digital inclusion through its initiatives. This country report particularly looks at the governance of internet in New Zealand. In this regard, various aspects relating to privacy, personal data, information security, and intermediary regulation have been looked into.

A. Digital Constitutionalism and Internet Governance

Introducing Digital Constitutionalism

1. How can we define Digital Constitutionalism?

Digital Constitutionalism has been defined as, "a common term to connect a constellation of initiatives that have sought to articulate a set of political rights, governance norms, and limitations on the exercise of power on the internet, and/or the notion aiming at establishing a normative 'Constitutional' framework for the protection of fundamental rights and the balancing of powers in the digital environment."[1] Over the past few decades, the continuous development of digital technology and its disturbing impact on society has affected the equilibrium of the constitutional environment.

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

The key norms that *New Zealand's Constitution* revolves around are representative democracy, parliamentary sovereignty and the evolving and unwritten nature of its *Constitution*.[2] Some other pertinent constitutional principles are rule of law and separation of powers.[3] All people and institutions of power in New Zealand are to be accountable for their actions and should act within legal limits. A crucial aspect to the rule of law is an independent and impartial judiciary. Judicial decisions result in the development of common law, and courts are the only bodies that have the power to convict and imprison people.

Separation of powers is another significant Constitutional principle. Every branch of the government is required to perform those functions associated with its branch and cannot overreach into the boundaries of another branch. This principle seeks to prevent concentration of power in one branch of the government and institutes checks and balances that prevent abuse of power. In New Zealand, while the executive and legislative branches share a common membership, there are institutional safeguards that ensure accountability. Furthermore, the judiciary cannot be used as a tool to seek vengeance against one's political opponents. Representative democracy, parliamentary sovereignty, rule of law and separation of powers are some of the pertinent traditional constitutional concepts. To ground Digital Constitutionalism in these traditional concepts, it is pertinent for these aspects to be an innate part of a Digital Constitution.

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

A Digital constitutional model *for* the people should prioritize users' interest over that of digital platforms that seek to maximize their profits. Digital practices that violate fundamental constitutional principles such as the right not to be deprived of life, physical integrity of one's body, freedom from torture or cruel punishment, freedom from discrimination based on immutable characteristics, physical liberty, freedom of conscience, liberty, and procedural fairness should be deemed unconstitutional. Given the vast nature of the digital space, regulation of it is difficult. However, it is pertinent that platforms be held accountable for their actions, against the touchstone of constitutional principles.

A *by*-the-people model for Digital Constitutionalism can be advanced through ensuring that authoritative representatives are elected by way of universal suffrage. Given the novelty of the digital space as of right now,

---

[1] Lawrence Lessig, 'Digital Constitutionalism' (*Institute for Internet & the Just Society*) < https://www.internetjustsociety.org/digitalConstitutionalism>accessed 22 April 2021.

[2] Matthew S Palmer, 'New Zealand Constitutional Culture' (2007) Vol. 22, New Zealand Universities Law Review <file:///C:/Users/Anushya%20Ramakrishna/Downloads/SSRN-id1069061.pdf>accessed 17 April 2021.

[3] 'Fundamental Constitutional Principles and Values of New Zealand Law' (*Legislation Design and Advisory Committee*) < http://www.ldac.org.nz/guidelines/legislation-guidelines-2018-edition/Constitutional-issues-and-recognising-rights/chapter-4/ >accessed 21 April 2021.

there is no system of user representation in drafting policies with regards to digital platforms. Users do not have a say in the process of drafting such policies; rather it is elected representatives of the Legislature who make these policies. Ensuring the inclusion of users in digital policy drafting processes may not wipe out the dominance of digital platforms, but at least it shifts the extreme power imbalance in favour of users, to a certain degree.

Finally, an *of*-the-people model calls for digital platforms to be more competitive to ensure that users are given sufficient choices of appropriate quality. The domination by online monopolistic companies brings about exclusion within the digital space. The government is obligated to regulate these platforms and bring about inclusivity and visibility of other actors, which in turn brings about competition in the digital space.

Representativeness of Online Platforms

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

New Zealand has been forward-thinking in seeking to bring about digital transformation for its citizens. Its digital government model is focused on ensuring that people are put first. The government seeks to provide for all the needs of its citizens in a time of emerging technologies, data, and changes to government culture, practices, and processes. Apart from improving information technology (IT) systems and processes, the New Zealand government strives to use new mindsets, skillsets, technologies, as well as data to benefit the citizens and government, along with the economy. Through this initiative, the government strives to ensure that citizens can access personalised services where and when they need them, along with engaging in decisions about issues they are passionate about, and to trust in an transparent, open, and inclusive government.[4]

However, there is some critique of the government's efforts. New Zealand's government website status is fragmented and requisite information is provided on numerous websites. There are other pertinent issues created by New Zealand's e-government regime. They are in relation to access, relationships, society, regulation, worth and protection.[5] On the aspect of access, New Zealand faces an unequal access to the internet as well as social services. This demonstrates the socio-economic divisions that are prevalent there. This digital divide is between the rich and the poor as well as those living in urban and rural spaces.[6] Another facet in relation to the issue of access is with regards to the indigenous people. The Maori communities and leaders fear that the internet and e-government could affect their culture, rights, values, privacy and intellectual property.[7] On the relationship front, the government requires the feedback of players in the private sector as well as citizens. Through its digital government model, the New Zealand government should strive to bring about confidence and trust in the people and groups who benefit from it. It is seen that due to privacy and security issues, consumer trust and confidence is low. This is one of the aspects the government needs to work on.[8]

This report strives to shed light on how the government can meet the needs of the people in these changing times with the use of emerging technologies, data, and changes to government practices, cultures and process. Online platforms can be made more inclusive, representative and equal by ensuring that the digital sphere takes into consideration the differences that every user experiences, and accounting for it by way of the services they provide and in the mode that they provide it.

New Zealand's government has accepted that we live in a time of swiftly changing digital technologies that affect our work, access to entertainment, communication, and the world as seen by us.[9] Digital inclusion is "social inclusion in the 21st century that ensures individuals and disadvantaged groups have access to, and skills to use, Information and Communication Technologies and are therefore able to participate in and benefit from today's growing knowledge and information society."[10]

---

[4] 'Introduction to NZ's digital transformation' (*Digital.gov.nz*) < https://www.digital.govt.nz/digital-government/about-digital-government/introduction-to-nzs-digital-transformation/>accessed 12 October 2021.

[5] Eric Deakins and Stuart Dillon, 'E-Government Issues in New Zealand' (2002) ResearchGate < https://www.researchgate.net/publication/2534884_E-Government_Issues_in_New_Zealand/citations>accessed 12 October 2021.

[6] ibid.

[7] ibid.

[8] ibid.

[9] 'The Digital Inclusion Blueprint- Te Maher mot e Whakaurunga Matihiko' (*Digital.gov.nz*) < https://www.digital.govt.nz/assets/Documents/113Digital-Inclusion-BlueprintTe-Mahere-mo-te-Whakaurunga-Matihiko.pdf > accessed 7th July 2021.

[10] 'Digital Inclusion definition' (*Digital Inclusion Map*) < https://digitalinclusion.nz/about/digital-inclusion-definition/>accessed 12 October 2021.

New Zealand's digital inclusion blueprint includes four elements: access, motivation, skills and trust.[11] To bring about digital inclusion, the government has to play the role of connecting, supporting, leading and delivering, so as to ensure that everyone can participate, contribute and benefit from the digital world. For digital platforms to be more representative, all involved stakeholders need to be given a chance to participate on these platforms. With regards to equality, digital platforms need to ensure that their practices treat all people equally as well as provide their services equally to all.

Some of the issues of digital inclusion that the New Zealand government has faced was with regards to inequitable access to the internet. In an attempt to bridge this digital divide, the government sought to provide low-cost public access to the internet as well as computers at the community level.[12] Additionally, the government has implemented a 'Closing the Gaps' policy that strives to provide less-advantaged citizens with low-cost public access to public services.[13] Subsequently, to allay the fears of indigenous people, on the negative effects of a digital government model, the government will consider the intellectual property and cultural rights of the Maori community as well as include their local language on the government websites.[14]

These are some examples of how the New Zealand government is working to ensure that its digital government benefits all its citizens. While these measures may not be able to tackle the issues that a digital government model poses, it is a step in the right direction. Furthermore, it demonstrates the government's genuine desire to use the digital government model to benefit its citizens.

Open Source Intelligence

5. 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 (OSINT) ensures systemic collation, structuring and analysing of publicly available information. It can be used to increase productivity for corporations, recognize and mitigate existing or plausible risks and to avert crimes.

In New Zealand, there has been an attempt made to ensure open-source intelligence (OSINT) in the digital space. New Zealand is also one of the countries which has adopted strong Open Data policies. As a consequence of this, objective data that is made available on the internet rapidly increases.[15] 'OSINT New Zealand' is a digital platform on which databases have been made available that help citizens find useful information, such as judicial decisions, company-related information, intellectual property, lawyer database, doctor registration, COVID-wage subsidy and other such information. This allows for citizens to access relevant information more easily in the digital sphere.[16] Therefore, OSINT plays a significant role in ensuring that information that is found all over the internet is made available for citizens at one place.

Despite the benefits of OSINT, it is pertinent to regulate it to prevent misuse of the freely available information. Some principles that have been taken into consideration by New Zealand to control and regulate OSINT are respect for privacy, necessity, proportionality, least intrusive means, respect for freedom of expression, and legality.[17] The *Intelligence and Security Act* 2017 regulates government agencies and their oversight system.[18] While the internet space provides security threats, therefore, requiring the intervention of government agencies, it is pertinent to ensure that these agencies are not given unbridled power. Similarly, the OSINT space needs to be regulated with similar legal instruments that enhance the benefits and curbs the disadvantages of the same.

---

[11] ibid.
[12] ibid (n 5).
[13] ibid.
[14] ibid.
[15] Javier Pastor-Galindo, Pantaleone Nespoli, Felix Gomez Marmol, and Greorio Martinez Perez, 'The Not Yet Exploited Goldmine of OSINT: Opportunities Open Challenges and Future Trends' (2016) ResearchGate < https://www.researchgate.net/publication/338495014_The_Not_Yet_Exploited_Goldmine_of_OSINT_Opportunities_Open_Challenges_and_Future_Trends>accessed 12 October 2021.
[16] 'OSINT New Zealand' (*Open Source Intelligence New Zealand*) < https://www.osint.rocks/>accessed 12 October 2021.
[17] 'Obtaining and using publicly available information,' Ministerial Policy Statement <https://www.nzic.govt.nz/assets/assets/mpss/Ministerial-Policy-Statement-Obtaining-and-using-publicly-available-information.pdf>accessed 12 October 2021.
[18] 'Legislation' (*Government Communications Security Bureau*) <https://www.gcsb.govt.nz/about-us/legislation/>accessed 12 October 2021.

6. 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 Digital Constitution as an integrative model draws upon and comprehensively presents standards as opposed to grounding ideals, which would not be ideal.[19] While New Zealand does not have a written Constitution, other legal documents lay down grounding principles upon which the nation is built. These grounding ideals lay the foundation for future laws and regulations as a Constitution and its principles are expected to be a foundation for these future regulations and legislations. Comprehensive standards of law for Digital Constitutionalism would give rise to uncertainty in the instance that a situation arises that was not envisaged by lawmakers. Given the rapidly changing nature of the digital space, there is a very high probability of a such a situation arising as well.

For New Zealand to be able to balance the foundations of Digital Constitutionalism, the need to be dynamic and adaptable with the changing spectrum of the digital space as well as upholding grounding ideals, there is need for a governing legislation. A legislation lays down the boundaries within which Digital Constitutionalism and the surrounding space is grounded. A legislation would further provide a sense of stability in the fast-changing digital environment. Such a legislation would appropriately create a balance by ensuring that the provisions for Digital Constitutionalism are grounded in existing constitutional principles. Additionally, the legislation should account for the changing digital space and anticipate future events arising from it. This would combine being grounded in constitutional principles and creating legislative space to accommodate for future possibilities that the digital space could give rise to.

Competition Law and the Internet

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

The big-tech firms around the world have come under the scanner for violating antitrust laws. These laws seek to promote competition and protect consumers. Google, Facebook, Microsoft, Amazon, and Apple are often termed as the big-tech firms.[20] These companies together exert a higher level of influence in the information and technology world than any other company. To tackle the issues that these tech firms can give rise to, New Zealand has a *Commerce Act* of 1986.[21] This *Act* has numerous provisions like extraterritorial jurisdiction and prohibition on misuse of dominant power.

However, the primary issue that we run into is that the contents of the *Act* were not formulated with the internet in mind. To allow for rapid development in the world of the internet, the creators had "permissionless innovation"[22] in the initial years. This eventually led them to be self-regulating in nature as the industry progressed. It is primarily this reason why today we witness data breaches and privacy concerns as there is a lack of regulation. The 2019 report by the New Zealand Commerce Commission also suggested better legislation to deal with these issues. [23]

The big-tech firms have a certain monopoly in their respective spheres. While there has not been a definitive case that dealt with monopoly of the internet giants, we can look at a case of monopoly pertaining to the telecom sector to gauge the efficacy of the laws. In *Telecom Corp. of N.Z. Ltd. v. Clear Communications Ltd*,[24] while dealing with issue of monopoly, the privy council stated that "It cannot be said that a person in a dominant market position "uses" that position for the purposes of s 36 if he acts in a way which a person not in a dominant position but otherwise in the same circumstances would have acted." Although this judgment was criticised for its inability to prevent monopolistic tendencies in the market, it has been upheld in all the judgments that followed it. Hence, today a big tech company that occupies a position of monopoly in the

[19] Dr. Edoardo Celeste, 'What is Digital Constitutionalism' (*Digital Society Blog*, 31 July 2018) < https://www.hiig.de/en/what-is-digital-Constitutionalism/>accessed 12 November 2021.
[20] 'The Economics Of Big Tech' (*Financial times*) <https://www.ft.com/economics-of-big-tech> accessed 10 April 2021.
[21] Commerce Act 1986.
[22] 'What Is Permissionless Innovation? - Permissionless Innovation' (*Permissionless Innovation*) <https://permissionlessinnovation.org/what-is-permissionless-innovation/> accessed 9 April 2021.
[23] International Bar Association, 'New Zealand: Antitrust Update' (2020) <https://www.ibanet.org/Article/NewDetail.aspx?ArticleUid=E0367ACD-D955-4330-B070-EF8CB821ED6E> accessed 10 April 2021.
[24] [1995] NZLR 385 (P.C.).

market can continue to do so if they merely prove that they are not abusing the position. This can lead to serious barriers to entry for new entrants and lack of options for the consumers, inevitably leading to exploitative practices.

Hence to protect the interests of people and smaller tech firms, more elaborate safeguards and stricter regulation is necessary.

The Regional, constitutional and Transnational Aspects of a Digital Constitution

8. 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?

With the boom of the internet, many organizations have now come to play their part in protecting and promoting the 'internet rights' of people. NGOs like the Spark Foundation work towards advocating for equal rights for internet access. These NGOs work at the grassroot levels to educate and empower people who may not have access or be aware of their rights regarding the digital ecosystem.

Since these organizations are often underfunded, the higher responsibility is on the organizations under the central authority such as the human rights commission or the commerce commission. The judiciary is the main protector of rights of the citizens of a country. However, it is often witnessed that due to the division of subject matter, there is inconsistency in their judgements. Although the Supreme Court is the final court of appeal, having a consistent stance on issues can help to solidify certain rights. This can be achieved by better communication and consultation among the courts.

9. 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)?

New Zealand has three main laws that deal with the virtual world: The *Human Rights Act 1993*, *Article 14 of the New Zealand Bill of Rights Act 1990 (NZBORA)*, and the *Privacy Act*. Some provisions of these laws overlap with one's internet rights. However, with the ever-evolving nature of the digital ecosystem, these laws often seem inadequate to deal with the issues in their entirety.

There are three key issues where there is a need for innovation. Since the internet is not restricted by the physical borders of the world, oftentimes the jurisdiction becomes an issue. The second issue is that a substantive part of the internet is behind firewalls and cannot be accessed by everyone, often referred to as the dark web. [25] Any kind of illegal activity that takes place in this part of the internet becomes difficult to track. The last issue that requires development is of Net Neutrality which means that data should be treated equally.

With regards to the first issue, New Zealand has recently enacted the *Privacy Act*, *2020*.[26] It includes the feature of extending itself to extraterritorial activities. Even in a case wherein an individual or a company collects date or conducts business in New Zealand, they can be held accountable under the new *Act* irrespective of their place of residence. For the second issue, there are currently no laws in New Zealand that forbid a person from accessing the dark web[27] so it can get very difficult for the agencies to track activities on it. With regards to the last issue, while there are no net neutrality laws or regulations in New Zealand, it is not a threat. The telecommunications market is very competitive and even the biggest player, Chorus, is restricted to only selling to internet service providers and not directly to consumers.[28]

While privacy and net neutrality are a major concern around the world, New Zealand has been one of the few countries to actively engage with the subject matter and formulate laws to safeguard the interest of its citizens. However, owing to its dynamic nature, laws concerning the internet have to be regularly monitored and amended to keep up with the changing times.

---

[25] 'What Is The Dark Web? How To Access It And What You'll Find' (*CSO Online*, 2020) <https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html> accessed 12 April 2021.

[26] Privacy Act, 2020.

[27] Clayton R, "Is the Deep Web as Formidable as It Sounds?" (StuffApril 22, 2016) <https://www.stuff.co.nz/technology/digital-living/79192225/is-the-deep-web-as-formidable-as-it-sounds> accessed November 10, 2021.

[28] Katie Kenny, 'What Is Net Neutrality And Why Should New Zealanders Care About It?' (Stuff, 2018) <https://www.stuff.co.nz/technology/101255330/what-is-net-neutrality-and-why-should-new-zealanders-care-about-it> accessed 4 September 2021.

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

Different parts of the world ascribe different levels of importance to the values of speech, privacy, etc. The only plausible way to harmonize these frameworks is by focusing on certain core values and by encouraging cooperation. Harmony can be achieved by tackling all the issues that have so far been the reason for the ineffectiveness for similar such frameworks. We can consider the example of the European Union (EU). The *General Data Protection Regulation* (*GDPR)* that was adopted in 2016 addressed the regulation of data privacy concerns for the entire region of EU. It was based on the agreement of certain core principles of rights that the countries agreed upon.

By ensuring a stricter enforceability, aligning the intent and equal treatment of all stakeholders, one can find a way leading to an effective global Constitution. A number of examples such as the WTO can be looked at wherein the failure to comply with the norms can lead to sanctions. However, there are not attempts by New Zealand to be part of an initiative with multiple countries to harmonize the various national frameworks.

B. Human and Constitutionally Guaranteed Rights

Internet Users and Online Platforms

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

There exists a vast array of rights that a person possesses in the virtual world. Most of these principles also overlap with the Constitution of the country. Although New Zealand does not have a written Constitution, it has various legislations dealing with these rights.

Equality, freedom of speech and privacy are the three main themes of these rights. There have been numerous legislations passed in this respect to deal with them, namely, *Human Rights Act 1993*, *NZBORA*, and the *Privacy Act 1993*. There also exists plenty of other rights for citizens online which can be in the field of access, stability, intellectual property and transparency. As stated previously these legislations need substantive developments to better adapt to the virtual world.

2. Who can be defined as a netizen?

Netizen is a portmanteau of the words internet and citizen, essentially identifying anyone that uses the services of the internet.[29] However a more evolved meaning of the word indicates anyone that works towards the internet for the mutual benefit of everyone. Benefit here refers to an active good. It does not include someone not actively harming the internet but just using the internet. Anyone who merely uses the internet can be termed as a lurker and not a netizen.[30]

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

The term bad actor implies anyone misbehaving or creating trouble for others. With reference to its usage in New Zealand, we have seen after the Christchurch attack that it was used to describe people who were continuously resharing the videos of the shooter.[31] They also actively engage in illegal activities on the dark web as described above. Hence, taking this meaning of the word we can infer that bad actors cannot be termed as netizens as, while they are users of the internet, they are not benefiting it in any way.

4. 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?

The existing law in New Zealand does not regulate internet shutdowns, slowdowns and communication throttles. There is evidence that internet service providers (ISPs) block, throttle or deprioritise content that is outside a bundle.[32] Internet service providers are incentivised to do this to recover their 'costs' or otherwise

[29] Amelia DeLoach, 'What Does It Mean To Be A Netizen?' [1996] *CMC* <https://www.december.com/cmc/mag/1996/sep/callnet.html> accessed 10 April 2021.

[30] Daub A, "The Rise of the Lurker" (The New RepublicNovember 10, 2021) <https://newrepublic.com/article/157274/rise-lurker-joanne-mcneil-book-review> accessed November 10, 2021.

[31] 'Christchurch Shootings: 'Bad Actors' Helped Attack Videos Spread Online' (*BBC News*, 2019) <https://www.bbc.com/news/technology-47652308> accessed 10 April 2021.

[32] 'Network Neutrality in New Zealand' *(Internet NZ, June 2015)* <https://internetnz.nz/assets/Archives/Network_neutrality_discussion_document.pdf> accessed 17 September 2021.

enforce payment obligations upon content distributors in exchange for the efficient distribution of their content.[33]

The only known obligation that prevents internet service providers from doing so is the *Broadband Product Disclosure Code of Practice* developed by the Telecommunications Forum (TCF). Pertinently, this *code* only applies to members of the TCF, and membership of the TCF is not required in order to be an ISP in New Zealand. *The Broadband Product Disclosure Code of Practice* includes a transparency obligation under *Section 7.1.3(k)*. It imposes an obligation on internet service providers to have a traffic management policy which in turn would require them to disclose any arrangements that prioritised certain traffic kinds over another.

There are two important implications of the preceding paragraph. Due to the limited applicability of the *Broadband Product Disclosure Code*, there is no obligation on ISPs in New Zealand to not participate in internet slowdowns and throttles, Thus, it is important that guidelines applicable to the same are developed. However, TCF member companies represent over 95% of New Zealand telecommunications customers.[34] Thus, these transparency obligations arguably ensure that ISPs disclose any arrangements they enter into, which can be subsequently voided.

Social Media Councils

5. 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?

Article 19, a British human rights organisation, has advocated for the creation of social media councils. Social media councils, at the national level, would serve as an appellate body for content moderation decisions made by platforms. These national councils would be governed by a global code of principles, which would be applied within a local context.[35]

In New Zealand, there exists the New Zealand Media Council, an independent forum for resolving complaints relating to the traditional channels. This includes content of newspapers, magazines and periodicals (including their websites), online content of select broadcasters, etc.[36]

However, New Zealand officials have acknowledged that this regulation should extend to social platforms in new media regulations. The Department of Internal Affairs acknowledged that New Zealand media industry regulations are from a pre-internet era, and does not provide adequate protection against harmful content consumed in recent times.[37] It is necessary for New Zealand to develop its own norms for regulating social media companies before agreeing to apply a global code of principles. This is necessary because the global norms must also meet the social expectations of New Zealand.[38]

C. Privacy, Information Security, and Personal Data

Personal and Non-Personal Data

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

With the advent of Big Data, it is vital that government bodies take necessary steps to protect the data rights of their citizens. Data protection regulations ensure the security of individuals' personal data and regulate its collection, usage, transfer, and disclosure. Thus, when we enquire into a nation's data protection regulations, the foremost question to be asked is how expansively or narrowly it defines personal data. When it comes to New Zealand, it takes a very expansive approach. *Section 7 of the Privacy Act* defines 'personal information' as follows:

> **"personal information**—
>
> **(a)** means information about an identifiable individual; and

[33] ibid.

[34] 'About Us' (TCF, 15 July 2021) <https://www.tcf.org.nz/consumers/about-us/> accessed 19 October 2021.

[35] 'Social Media Councils: From Concept To Reality' (2019) <https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/gdpiart_19_smc_conference_report_wip_2019-05-12_final_1.pdf> accessed 20 July 2021.

[36] 'Independent Forum For Resolving Complaints' (*Media Council*, 2021) <https://www.mediacouncil.org.nz> accessed 20 July 2021.

[37] Stephen Parker, 'Social Platforms Should Be Captured In New Media Regulations – Officials' (*Newsroom*, 2021) <https://www.newsroom.co.nz/media-regs-to-capture-social-platforms> accessed 20 July 2021.

[38] Susan Etlinger, 'What's So Difficult about Social Media Platform Governance?' (*CIGI 28 October 2019*) <https://www.cigionline.org/articles/whats-so-difficult-about-social-media-platform-governance> accessed 19 September 2021.

(b) includes information relating to a death that is maintained by the Registrar-General under the Births, Deaths, Marriages, and Relationships Registration Act 1995 or any former Act (as defined in section 2 of the Births, Deaths, Marriages, and Relationships Registration Act 1995)"

As per *Section 7 of the Privacy Act*, personal information means any information about an identifiable individual. Identifiability here includes any information that, depending on context, has a sufficient connection to that individual. Since the enquiry is contextual, it takes a broader sweep and also includes information that may be used if combined with other information to identify people. Even the exceptions to this definition of personal information are construed narrowly such as personal information that is already public knowledge.[39] For example, the dataset of marriage celebrants on data.govt.nz includes contact details for these people; however, this data is public knowledge and already released publicly elsewhere.[40]

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

New Zealand has a robust mechanism for the regulation of non-personal data or open data. For this it uses *the New Zealand Government Open Access and Licensing (NZGOAL)* framework and the *Copyright Act*. The *NZGOAL* lays down policy principles that should be followed for the dissemination of data. While open access is the default rule for dissemination of information, that is subject to restrictions found in *Article 24*. These *inter alia* include compliance with the legislation or government policy, protecting IPR, and public interest. On top of this, dissemination of non-personal data is governed by moral rights. Moral rights are statutory rights in the Copyright Act that are personal to the authors or other creators of original works. They are distinct from the exclusive and economic property rights conferred on the owners of copyright works. For example, in case of literary works, two relevant moral rights would be the right to be identified as author (*Section 94*); and the right to object to derogatory treatment of a work (*Section 98*).

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?

In end-to-end encryption only the sender and the recipient of certain information can access it. However, multiple law enforcement agencies worldwide have been calling for tech companies to create backdoors in their encryption systems, thus providing the state with access to the content otherwise protected by end-to-end encryption. One such country is New Zealand who recently joined the Five Eyes countries to call for backdoors to end-to-end encryption.[41] The back door is being justified using risks posed to public safety in particular to vulnerable groups in case of unbreakable encryption technology. However, this move by the New Zealand government has been widely criticised as it did not hold any public consultations before joining the Five Eyes.[42] This move is not desirable for New Zealand who is otherwise pro-data protection. Backdoor encryption is always posed as the 'good guy' for the law enforcement; however, it is debatable because there is always a risk of third-party access. Traceability might diminish user security and privacy because to enable this function the service providers must be forced to access the private content of the user's communications which can be a cause for concern. Further, this can also diminish trust of the users and consequently diminish the internet's utility.[43]

Breaking encryption can reduce confidence in e-commerce, independent journalism, whistleblowing and many other sectors or scenarios where the confidentiality and integrity of information is essential. Further, this move may enable cyber and cyber-related crimes. Importantly, the government has not yet brought in specific anti-encryption law and joining the Five Eyes can be viewed as an attempt to facilitate discourse on the subject.[44]

---

[39] 'What Is Personal Information And The Privacy Act? - Data.Govt.Nz' (*Data.govt.nz*, 2021) <https://www.data.govt.nz/manage-data/privacy-and-security/what-is-personal-identifiable-information-and-the-privacy-act/> accessed 19 April 2021.
[40] ibid.
[41] Matthias, 'Any Encryption Backdoor Would Do More Harm Than Good' (Tutanota, 28 August, 2020) <https://tutanota.com/blog/posts/why-a-backdoor-is-a-security-risk/> accessed 5 September, 2021.
[42] ibid.
[43] PTI, 'Traceability on Digital Platforms May Diminish Users Security, Privacy: Internet Society' (18 January, 2020, Economic Times) <https://brandequity.economictimes.indiatimes.com/news/digital/traceability-on-digital-platforms-may-diminish-users-security-privacy-internet-society/80327420> accessed 18 April, 2021.
[44] Matthias n(1).

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

New Zealand has a good track record with ensuring compliance with data protection regulations and privacy statutes even during times of crises. This is clear from New Zealand's treatment of privacy concerns during the Covid-19 pandemic. The country preferred relying on lockdowns to using personal data to deal with the pandemic. In fact, the NZ Covid Tracer App based itself on the consent model of privacy and facilitated an opt-in option. The Privacy Commissioner appointed as per the *Privacy Act* also published guidelines to address privacy concerns.[45] He suggested a balancing test in that personal information regarding someone's health should remain private unless there is a public health risk. So, it becomes important in such times of crisis to place a balance between rights and other concerns posed by any crisis so that the measures implemented do not become excessive, arbitrary or discriminatory.

Intelligence Agency

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

New Zealand regulates the operation of intelligence agencies online using the *Privacy Act* and the *Intelligence and Security Act 2017*.

As per the *Privacy Act*, intelligence agencies are authorised to use and disclose information that is reasonably required for the agency to perform any of its functions. Further, the *Information Privacy Principles 2, 3, and 4(b)* do not apply to personal information collected by an intelligence and security agency. Furthermore, intelligence agencies are also regulated by a special procedure provided within *Section 95*.

Additionally, as per *Part 7 of the Intelligence and Security Act 2017*, ministers responsible for the security and intelligence agencies must issue ministerial policy statements (MPS) to provide guidance on specific matters that security agencies must apply. The MPSs issued so far include "principles of legality, necessity and proportionality, as well as the need for effective oversight".[46] Further, the complaints filed against intelligence agencies will be adjudicated upon by the Inspector General of Intelligence and Security (IGIS).

D. Intermediary Regulation

Online Harms and Netizens

1. How do we define online harms?

Internet has become an integral part of everyone's life. With its growing presence, it is important to analyse the real harms which people can face. Online harm is online behaviour which may cause emotional or physical harm to a person.[47] Internet can be used for illegal activities, terrorism, undermine civil discourse, bully or abuse people which can have serious consequences.

2. How should community guidelines for online platforms be drafted, disseminated, and enforced?

The Ministry for Business, Innovation and Employment (MBIE) has recognised that the quality of regulatory systems employed by the government has a major impact on the lives of all New Zealanders.[48] Hence, participation of the community in drafting, dissemination and enforcement of community guidelines is

[45] John Edwards, Privacy Commissioner "Privacy versus Security – the False Dichotomy and the Myth of Balance" speech to the New Zealand Institute of Intelligence Professionals Annual Conference (15 July 2015).
[46] ibid.
[47] Alex Hern, 'Online Harms Bill: Firms May Face Multibillion-Pound Fines For Illegal Content' (The Guardian, 15 December 2020) <https://www.theguardian.com/technology/2020/dec/15/online-harms-bill-firms-may-face-multibillion-pound-fines-for-content> accessed 18 April, 2021.
[48] New Zealand Government, 'The Best Practice Regulation Model: Principles and Assessments' (2012) <http://regulatoryreform.com/wp-content/uploads/2015/02/New-Zealand-Best-Practice-Regulation-Model-2012.pdf> accessed 18 April, 2021.

necessary as they are the active stakeholders. In present day New Zealand, there is no legislation which provides an advisory framework under which online harms can be countered using community guidelines.

The social context of the region must be taken into consideration while formulating community guidelines. Especially after incidents like the March 2019 terrorist attack at Christchurch,[49] minority communities must be given priority and their rights must be taken into consideration, when drafting the community guidelines.[50] Recently, the government of New Zealand amended the *Films, Videos, and Publications Classification Act, 1993* to allow for necessary and urgent mitigation of harms caused by any objectionable online publications.[51] Under the amended *Act*, a chief censor will assume certain powers to make any interim classification assessments regarding any publication in situations where of objectionable content is injurious to the public good. Furthermore, the 'safe harbour' provisions provided under the *Act* would not apply, which would prevent the host from being prosecuted.[52] Furthermore, since 2010, the New Zealand government has been using the Digital Child Exploitation Filtering System (DCEFS).[53] This is an opt-in filter which blocks a list of pages and websites that contain objectionable material involving children.

Reporting mechanisms, which allow flagging harmful content, should be made available and must be accessible for all users. Ease of access and transparency to track the reports can also help in building a reliable and safe internet space.[54] Such services are provided by Netsafe, an online safety organisation based in New Zealand.[55] Netsafe provides information regarding the various reporting systems for prominent online platforms and also investigates complaints about digital harassment.

Improvement in the policies to moderate content and prevent harmful communications is highlighted by initiatives like Christchurch Call and the Global Internet Forum to Counter Terrorism. Christchurch Call, which was adopted after the Christchurch attacks, signed by 18 governments and eight companies, and later endorsed by the UNESCO and Council of Europe, is a commitment by governments to eliminate violent extremist content online.[56]

Furthermore, numerous scholars indicate how online platforms and their community guidelines should align with international human rights standards. Some recommendations talk about how there should be more involvement of the relevant stakeholders, or a need to strengthen the position of large incumbents, and aim for limited intervention to protect privacy of individuals.[57] The latest amendment to the *Films, Videos, and Publications Classification Act, 1993* seems like a positive step forward as the government takes on the role to limit harmful content online through chief censors and also places certain liability on the host to moderate their content. Nevertheless, there is always a greater need for transparency and governments should be more proactive in trying to adhere to the international human rights standards.

3. 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?

New Zealand follows a safe harbour model which in highlighted in the *Harmful Digital Communications Act, 2015*.[58] This *act* provides for safe harbour provisions contained in *Sections 23 to 25* which limit the liability of the hosts for harmful content posted by any users. However, the host can insulate themselves from civil and criminal liabilities provided they administer a specific process when they receive a complaint regarding any

[49] 'Christchurch Shootings: 49 Dead in New Zealand Mosque Attacks' (BBC News, 15 March 2019) <https://www.bbc.com/news/world-asia-47578798> accessed 18 April, 2021.
[50] Rima Athar, 'From impunity to justice: Improving corporate policies to end technology-related violence against women' (APC 2015).
[51] Asha Barbaschow, "NZ introduces Bill to Block Violent Extremist Content" (ZD Net, 26 May, 2020) <https://www.zdnet.com/article/new-zealand-introduces-bill-to-block-violent-extremist-content/> accessed 12 September, 2021.
[52] Films, Videos, and Publications Classification (Urgent Interim Classification of Publications and Prevention of Online Harm) Amendment Bill, *2020*, "It would ensure online content hosts can be prosecuted for hosting objectionable content if they are liable for doing so".
[53] Department of Internal Affairs, 'Censorship DCEFS Public Information Pack', https://www.dia.govt.nz/Censorship-DCEFS-Public-Information-Pack#3.
[54] Carly Nyst, 'Internet intermediaries and violence against women online' (APC 2014).
[55] Ombudsman: Fairness for All, 'Netsafe' <https://www.ombudsman.parliament.nz/others-who-can-help/complaints-a-z/netsafe> accessed 19 April, 2021.
[56] 'Christchurch Call' <https://www.christchurchcall.com/christchurch-call.pd> accessed 18 April 2021.
[57] Mathias Vermeulen, 'Online Content: To Regulate or Not to Regulate – Is that the question?' (APC 2019) <https://www.apc.org/sites/default/files/OnlineContentToRegulateOrNotToRegulate.pdf> accessed 21 September 2021.
[58] Harmful Digital Communications Act, 2015, s. 23.

harmful digital communication. The Act does not require the host to remove the content immediately. It only requires them to notify the author and request them to remove the content. The host has the option to remove the content only when the author does not respond within 48 hours. Hence, hosts are for most parts' immune from any liability from third-party user generated content.[59] In 2014, a New Zealand court in *Murray v. Wishart*[60] ruled that the host will only be liable when they have actual knowledge about the harmful content and fail to remove them within reasonable time.[61] Hence, if the author denies to remove the content, the liability shifts to the author to prove why the content was not harmful.

There are some positive aspects of this *Act*. Firstly, an obligation is placed on the host to ask the authors to remove the content themselves. It also provides the author with an opportunity to express why they think the content should not be removed. Additionally, the *Act* gives an explicit length of time, 48 hours, to remove the content which reduces legal uncertainty during the safe harbour process.[62] Secondly, it guards freedom of expression, because it provides the author the opportunity to defend their ideas and it recognises that simply because some content offends some people doesn't make it *ipso facto* a 'Harmful Communication'.[63]

However, the problem with such an approach is that hosts are incentivised to err on the side of caution by removing content which will not necessarily attract any liability and not challenging any take down request. This could possibly result in a chilling effect and harm free speech. Hence, rather than relying on the hosts, the government should take up the initiative to regulate harmful content. The government should regulate keeping in mind the international human rights standards, privacy concerns, and rights like freedom of speech.

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

The Parliament of New Zealand enacted the *Harmful Digital Communications Act* in 2015 to deter, prevent and mitigate harm caused by individuals through digital communications as well as provide victims of harmful digital communications an efficient and quick means of redressal. The Act defines digital communications as any form of electronic communication and applies to any text message, writing, photograph, picture, recording or other matter communicated electronically. *Section 6* of the Act lays down the parameters for problematic user generated content and adopts 10 communication principles in this regard. The first principle laid down is that a digital communication should not disclose sensitive personal facts about an individual. The second principle laid down says that a digital communication should not be intimidating, threatening or menacing. The third principle says that a digital communication should not be grossly offensive. In order to determine whether the said communication is grossly offensive, the standard of a reasonable person in the position of the affected individual is applied. The fourth principle says that a digital communication should not be obscene or indecent. The fifth principle says that a digital communication should not be used to harass an individual. The sixth principle says that a digital communication should not make a false allegation. The seventh principle says that a digital communication should not contain matter that is published in a breach of confidence. The eighth principle says that a digital communication should not encourage or incite anyone to send a message to an individual for the purpose of causing harm to the individual. The ninth principle says that a digital communication should not encourage or incite an individual to commit suicide. The tenth principle says that a digital communication shouldn't denigrate an individual by reason on their race, colour, ethnic or national origins, religion, gender, sexual orientation or disability. [64]

Under the *Act*, if a digital communication violates one or more of the 10 principles, then the individual affected can move to the District Court. The District Court is empowered under the *Act* to grant interim orders under *Section 18* or *Section 19*. *Section 6(2)(a)* requires that the approved agency, in exercising their powers, must take into account the communication principles laid down in the *Act*. [65]

Another legislation relevant here is the *Films, Videos, and Publications Classification Act 1993* which was amended in 2020. On March 15, 2019, a terrorist attack against two mosques in New Zealand was live-

[59] Ministry of Justice, 'Safe Harbour Provisions' <https://www.justice.govt.nz/courts/civil/harmful-digital-communications/safe-harbour-provisions/> accessed 21 September 2021.
[60] Murray v Wishart [2014] NZCA 461.
[61] ibid.
[62] Stephanie Frances Panzic, 'Legislating for E-Manners: Deficiencies and Unintended Consequences of the Harmful Digital Communications Act'< http://www.nzlii.org/nz/journals/AukULawRw/2015/11.pdf>.
[63] ibid.
[64] Section 4, Harmful Digital Communications Act.
[65] Limits on Freedom of Expression' <https://www.loc.gov/law/help/freedom-expression/newzealand.php#_ftn39> accessed 18 April 2021.

streamed for 17 minutes on Facebook. Fifty-one people were killed and 50 were injured and the live stream was viewed around 4000 times before it was removed. This attack made it clear that there was a threat of violent and extremist content being published online. Two months after this incident, New Zealand Prime Minister Jacinda Arden and French President Emmanuel Macron brought together other heads of state and government to adopt the Christchurch Call. The Christchurch Call is a commitment by governments and technology companies to eliminate terrorist and violent content online. While it recognizes that a free, open and secure internet offers benefits to society, it also believes that no one has the right to create and share terrorist content online. [66]The Christchurch incident demonstrated the difficulties faced in removing the problematic content from the online platform. As a result, the *Films, Videos and Publications Classification (Commercial Video-on-Demand) Amendment Act* was brought in to allow for urgent prevention and mitigation of harms caused by objectionable publications. The *Act* makes live streaming of objectionable content a criminal offence, which was not prior to this amendment. The *Act* also confers additional authority on the Chief Censor to take swift action and make interim classifications of publications which have objectionable content if it is injurious to public good. The *Act* also authorises an inspector of publications to issue a take-down notice for objectionable content online. Take down notices can be issued to an online content host directing the removal of a specific link so that it is no longer viewable in New Zealand. In case an online content host does not comply with the takedown notice, they will be subject to a civil pecuniary liability. The *Act* also facilitates the setting up of mechanisms for filtering objectionable content in the future. In New Zealand, the only government-backed web filter is currently designed to block child sexual exploitation material. The *Act* facilitates the establishment of more government backed filters in the future if they are desired. [67] [68]

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

Online platforms were earlier viewed as platforms that merely enable individuals to share and publish content. Platforms were seen as a figurative blank sheet of paper on which anyone can write anything. They would refuse to hold any accountability over the content shared and published as they were merely facilitating exchanges between users. [69]However, as the role and reach of social media in sharing and disseminating information increases, platforms cannot continue to refuse taking accountability for content published. In the context of fake news, social media has practically become news media, and their responsibility over the information disseminated must increase accordingly.[70]

New Zealand's action on addressing the issue of fake news is limited to fake news propagated during election campaigning. During the 2020 election campaign, New Zealand's prime minister, Jacinda Arden announced that her party would sign up to Facebook's advertising transparency tool to fight misinformation. She said, "I don't want New Zealanders to fall into the trap of the negative fake news style campaigns that have taken place overseas in recent years".[71] Facebook's ad transparency tools were set in motion after the 2016 US election, and they allow voters to see who is behind paid advertising on Facebook and how much had been spent on it. The prime minister said that by being transparent about who was behind ads, there would be a flow-on effect on other parties to ensure they are accurate too.

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.]

The Parliament of New Zealand enacted the *Harmful Digital Communications Act* in 2015 to deter, prevent and mitigate harm caused by individuals through digital communications. The Act defines digital

[66] 'Christchurch Call' <https://www.christchurchcall.com/> accessed 18 April 2021.
[67] New Zealand Bills' <http://classic.austlii.edu.au/nz/legis/bill/fvapcicopapoohab20201200/> accessed 18 April 2021.
[68] NZ's new internet laws: Censorship or necessary for our safety?' *New Zealand Herald* (10 June 2020) https://www.nzherald.co.nz/nz/nzs-new-internet-laws-censorship-or-necessary-for-our-safety/B2EOPKF4VBTU5S642DLAQAKLIU/.
[69] Niam Yaraghi, 'How should social media platforms combat misinformation and hate speech?' (Brookings, 9 April 2019) <https://www.brookings.edu/blog/techtank/2019/04/09/how-should-social-media-platforms-combat-misinformation-and-hate-speech/> accessed 18 April 2021.
[70] Niam Yaraghi, 'How should social media platforms combat misinformation and hate speech?' (Brookings, 9 April 2019) <https://www.brookings.edu/blog/techtank/2019/04/09/how-should-social-media-platforms-combat-misinformation-and-hate-speech/> accessed 18 April 2021.
[71] New Zealand PM commits to 'positive' election campaign, warns of fake news' <https://www.reuters.com/article/us-newzealand-politics-ardern-idUSKBN1ZM0DX>.

communications as any form of electronic communication and includes any text message, writing, photograph, picture, recording or other matter communicated electronically. [72] Online content hosts, in relation to a digital communication, refer to the person who has control over part of the electronic retrieval system, such as an online application or a website on which communication is posted and can be accessed by the user. [73] The *Harmful Digital Communications Act, 2015* provides safe harbour provisions contained in *Sections 23 to 25* to limit hosts' liability for harmful content posted by users provided the hosts follow a specified process.

Section 24 lays down in detail the process for obtaining protection against liability for specific content online. *Section 24(1)* says that no civil or criminal proceedings can be instituted against an online content host if the host receives a notice of complaint about the specific content and complies with the provisions of *Section 24(2*). *Section 24(2)* requires that the host must inform the author of the complaint. This involves providing the author of the specific content with a copy of the notice of complaint and notifying the author of their need to submit a counter-notice to the host within 48 hours after receiving the complaint. In case the host is unable to contact the author after taking reasonable steps to do so, then the host must either disable or take down the specific content within 48 hours of receiving the complaint. In the situation that the host receives the counter-notice of the author consenting to the removal of the specific content, then the host must take down or disable the content as soon as it is practicable. In the other situation that the author in their counter-notice refuses to consent to the removal of the specific content, the host must leave the content in place and notify the complainant with the author's decision. In case the author fails to submit a valid counter-notice, then the host must take down the content as soon as it is practicable but not later than 48 hours after notifying the author. *Section 24(3)* and *24(4)* lay down the requirements of a notice of complaint and requirements of a counter-notice. *Section 24(5)* protects the privacy of the complainant and author and prohibits the online content host from disclosing any personal information about the complainant and author unless it is by the order of a District Court Judge or a High Court Judge.

Section 25 of the *Act* contains further provisions relating to the liability of the online content host. Section *25(1)* allows the approved agency to lodge a complaint under *Section 24* on behalf of the complainant and provide assistance to the complainant. The composition, functioning and scope of the 'approved agency' is defined under *Sections 7 to 10* of the *Act*. The approved agency is a person or organization or any department or any crown entity appointed by the governor general to assist in the process of resolving a complaint. The powers and functions of the approved agency include receiving and assessing complaints, investigating them, and resolving complaints. *Section 25(2)* does not allow the online host to seek the protection of *Section 24* if the host does not provide an easily accessible mechanism for the user to contact the host about the specific content. *Section 25(3)* also prevents an online host from taking the protection of *Section 24* if the specific content has been published on behalf or at the direction of the online host.[74]

The safe harbour protections are therefore offered to platforms only if they strictly comply with the procedure laid down in the *Act*. The online platform must therefore fulfil all their obligations under the *Act* in order to claim protection from liability. At the same time, the safe harbour protections are not available to hosts in case the platform violates criminal name suppression orders and publishes the name of the concerned person. Similarly, no exemption from liability is allowed if the platform publishes details about bail hearings, which is prohibited. Further, if any enactment explicitly overrides the safe harbour protections, then the platform cannot claim such immunity under this *Act*. While the safeguards under the Act are wide, the platforms must strictly comply with their obligations in order to claim immunity.

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?

The New Zealand Initiative and InternetNZ released a report on the state of regulation facing the technology sector in 2017 titled 'Analog Regulation, Digital World'. The New Zealand Initiative is an independent public policy think tank involved in developing policies that work for all New Zealanders. InternetNZ is a non-profit and open membership organization whose vision is for a better world through a better internet. The report stresses that with the increasing pace of technological change, New Zealand's

[72] Section 4, Harmful Digital Communications Act, 2015.
[73] ibid.
[74] Harmful Digital Communications Act, 2015.

ability to adapt to new technology depends on whether their regulations can keep pace. If they fail to keep pace, New Zealand will be left behind.[75]

New Zealand's experience with the 2019 Christchurch attack demonstrates the insufficiency of their previous approach towards dealing with violent content online. Although the video showing a terrorist shooting 50 people in a mosque was taken down by Facebook on the notice by authorities, there were several copies made by users which could bypass Facebook's algorithm which were circulated even months after the attack.[76] After this incident, Prime Minister Jacinda Arden said that she was looking for a meaningful change in the country's social media laws. The prime minister called on social media platforms to do more to fight terrorism. She said that people could not simply sit back and accept that these platforms take no responsibility for the content that is published. [77]She said, "social media platforms were publishers, and not merely the postman", and remarked that there cannot be a situation where these platforms take no responsibility.[78] [79] *The Films*, *Videos*, *and Publications Classification Act*, *1993* was proposed to be amended to introduce new measures to be able to swiftly tackle any objectionable content published online. This included making live streaming of objectionable content a criminal offence and also giving the Inspector of Publications more power to issue take-down notices of objectionable content, failing which the online content host will face civil liability.[80]

The introduction of the amendment to the *Films*, *Videos*, *and Publications Classification Act*, *1993* would allow for a swifter mechanism to tackle objectionable online content. This vests authority in the Inspector of Publications to take immediate action to remove such objectionable content. After the Christchurch attack incident, the government's approach, as evidenced by the prime minister's statements, shifted towards holding social media platforms accountable for the content on their platforms.

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?

On March 15, 2019, a terrorist had strapped a camera to his chest and began a Facebook live stream as he entered the Al Noor Mosque in Christchurch, New Zealand with an assault rifle and murdered 50 people. The video was quickly reported to Facebook by authorities and it was taken down. However, by this time, there were several copies made and reposted on social media platforms. Within hours, thousands of versions of the video were re-uploaded by users onto Facebook, Twitter and YouTube. Facebook revealed that in the first 24 hours of the video being uploaded, the video was uploaded by different users at least 1.5 million times and around 1.2 million of them were blocked by Facebook before they could be uploaded onto the platform. Facebook's inability to deal with this situation shows the fallibility of artificial intelligence moderation and any human content moderation. Even 36 days after the attack, Facebook was hosting videos of the attack on its own platform as well as on Instagram. Some of the videos were trimmed down to shorter lengths than the original video. Some versions of the attack video on Facebook were screen recordings of the video playing on the attacker's profile, while some were captures of someone watching the attack on Twitter. This demonstrates the number of permutations of the footage that continued to exist online, even after Facebook had removed the original clip.

As a response to this incident, Prime Minister Jacinda Arden said that she was looking for a meaningful change in the country's social media laws and was taking time to work out proposals. Shortly after the incident, the prime minister called on social media platforms to do more to fight terrorism. She remarked that social media platforms were publishers, and not merely the postman and said that there cannot be a situation where these platforms take no responsibility for the content published.[81] [82]

After the Christchurch attack, the New Zealand government appointed a commission called the Royal Commission of Inquiry with the task of investigating the terror attack and making recommendations to the government. The report made 44 recommendations including amending *the Films*, *Videos and Publications*

[75] <https://www.nzinitiative.org.nz/assets/Uploads/DigitalRegs-Report-Summary.pdf> accessed 18 April 2021.
[76] Alex Hern, 'Facebook and YouTube defend response to Christchurch videos' *The Guardian* (19 March 2019).
[77] Calla Wahlquist, 'Ardern says she will never speak name of Christchurch suspect' *The Guardian* (19 March 2019).
[78] Alex Hern, 'Facebook and YouTube defend response to Christchurch videos' *The Guardian* (19 March 2019).
[79] Calla Wahlquist, 'Ardern says she will never speak name of Christchurch suspect' *The Guardian* (19 March 2019).
[80] < http://classic.austlii.edu.au/nz/legis/bill/fvapcicopapoohab20201200/> accessed 18 April 2021.
[81] Alex Hern, 'Facebook and YouTube defend response to Christchurch videos' *The Guardian* (19 March 2019).
[82] Calla Wahlquist, 'Ardern says she will never speak name of Christchurch suspect' *The Guardian* (19 March 2019).

Classification Act 1993.[83] The key changes proposed by the *Films, Videos, and Publications Classification (Urgent Interim Classification of Publications and Prevention of Online Harm) Amendment Bill* include making the livestreaming of objectionable content a criminal offence. Live streaming refers to the online transmission of events in real time. The criminal offence of live streaming brought about by this *Act* applies only to the individuals who live stream the content. It does not hold the online content hosts that provide the infrastructure liable for the livestream. Another important feature of the proposed *Bill* is the power to issue take-down notices for objectionable online content. The Inspector of Publications is empowered to issue a take-down notice to an online content host directing the removal of the objectionable content. The online content host must comply with the take down notice as soon as it is reasonably practicable. In case the online content host fails to comply with the notice, then they will face civil liability.[84]

Another proposed reform by the *Bill* is the non-applicability of the safe harbour provisions in the *Harmful Digital Communications Act, 2015* in case of objectionable online content. *Section 24* of *the Harmful Digital Communications Act* protects online content hosts from liability for the content published by users if they follow certain steps when a complaint is made. The *Bill* proposes to exclude the applicability of the safe harbour clauses to ensure online content hosts are prosecuted for objectionable online content if they are held liable for doing so.[85]

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?

Almost every online platform has its own set of community guidelines and moderation policies. Even government ministries are engaged in providing the community with information through accounts on social media and have their own guidelines. For instance, the New Zealand Ministry of Health provides information through accounts on Facebook and Twitter and declares that it reserves the right to determine what constitutes inappropriate content, remove or edit such inappropriate content and also reserves the right to ban users from its social media communities. It also declares that it may delete posts that contain racist, sexist, homophobic, defamatory statements, misinformation, nudity, pornography or child abuse and content that advocates illegal activity.[86] The New Zealand Health Ministry provides a mechanism for users to contact the pages if there are any posts that the users feel violate the community guidelines.

When using a social media platform, while it is necessary to comply with the community guidelines of the platform, local laws should also be paid attention to. For instance, in New Zealand, a social media platform should ensure that it is not inadvertently breaching its obligations under the *Gambling Act, 1993*, or under the *Privacy Act 1193*, or under the *Unsolicited Electronic Messages Act 2007* or the *Advertising Standards Authority's rules*.

As the position stands in New Zealand, community guidelines by online platforms have to be mandatorily complied with by users, failing which the platforms have the right to delete the posts, or even ban users from using their platforms. At the same time, local laws also have to be complied with. Community guidelines are drafted keeping in mind the interests of various stakeholders and existing laws—local and international—and there hasn't yet arisen a situation where such guidelines are at conflict with other laws. Community guidelines are drafted keeping in mind existing rights and obligations under other laws and are generally seen as reasonable and acceptable standards to create a safe environment for users.

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?

The controversy regarding control of advertising has two sides, on one side, it is believed that in democratic countries that guarantee free speech, businesses should be allowed to publish content without being

[83] 'New Zealand to strengthen hate speech laws following Christchurch terror attack report' <https://www.jurist.org/news/2020/12/new-zealand-to-strengthen-hate-speech-laws-following-christchurch-terror-attack-report/> accessed 19 April 2021.

[84] < http://classic.austlii.edu.au/nz/legis/bill/fvapcicopapoohab20201200/> accessed 18 April 2021.

[85] < http://classic.austlii.edu.au/nz/legis/bill/fvapcicopapoohab20201200/> accessed 18 April 2021.

[86] 'Social Media Community Guidelines' <https://www.health.govt.nz/about-site/social-media-community-guidelines> accessed 19 April 2021.

restricted. On the other hand, some advertisements might have a negative impact on consumers' health, safety and overall wellbeing. In order to ensure that advertisements are legal, decent and truthful, self-regulation of the advertising industry through agreeable standards has been undertaken across countries.

Internationally, there have been self-regulatory codes and standards regulating advertisements since the early 1920s. In New Zealand, the committee of Advertising Practice was established by the New Zealand Broadcasting Commission, the Newspaper Publishers association as well as the Accredited Advertising Agencies Association in 1973. It was later renamed as the Advertising Standards Authority.[87] The objectives of the Advertising Standards Authority are threefold: Firstly, it seeks to maintain at all times and in all media, a proper and generally acceptable standard of advertising to ensure that advertising is not misleading or deceptive, either by statement of implication.[88] Secondly, it seeks to establish and promote an effective system of voluntary self-regulation. [89] Thirdly, it seeks to establish and fund an Advertising Standards Complaints Board.[90] The Advertising Standards Authority has, in consultation with advertisers, agency, media and the public, developed the *Advertising Standards Code*. In addition to this there are specific codes for advertising in the following sectors: Alcohol, Children and Young People, Finance, Therapeutic and Health, and Gambling.[91]

The *Advertising Standards Code* was brought into existence in 2018 with the purpose of ensuring that every advertisement is responsible, legal, decent, honest, truthful and respects the principles of fair competition so that the public may have confidence in advertising.[92] Under this *code*, the definition of 'advertisement' and 'advertising' includes any message controlled either directly or indirectly by the advertiser expressed in any language and communicated in any medium with the intent to influence the behaviour, opinion, or choice of those to whom it is addressed. [93]This *code* applies to all advertisements placed in any form of media. The code consists of principles, rules and guidelines. Principles lay down the standards expected to be followed in advertising. Rules give examples of how the principles are to be interpreted and applied and guidelines give information and examples to explain a rule.[94]

The first principle is that of social responsibility. This requires that advertisements should be prepared and placed with a due sense of social responsibility to consumers and society. There are nine rules enumerated under this principle. The first is that of privacy. This says that advertisements may only refer to or portray information that is publicly available. The second is that of consent. This requires that advertisers have due permission from the consumer before they engage in direct advertising communications. The third is that of decency and offensiveness. This prohibits advertisements from containing anything that may be degrading, indecent, exploitative or likely to cause harm, offence, or hostility. The fourth rule prohibits exploitation of children and young people and prevents advertisements from portraying anyone who is under 18 years of age in any way that is inappropriate or exploitative. The fifth rule is that advertisements must not encourage practices that are unsafe. The sixth rule is that advertisements should not show violent or anti-social behaviour. The seventh rule prohibits showing fear or distress without a proper justification. The eight rule prohibits advertisements from undermining the value of health and well-being and the ninth rule prohibits advertisements from depicting or encouraging environmental degradation. The second principle is that of truthful presentation which requires that advertisements be truthful, and not misleading. There are eight rules enumerated under this principle. The first rule is that advertisements should be identifiable. The second rule is that advertisements should not be misleading, deceiving, confusing, etc. The third rule is that data should not be used by advertisers in a manner that is deceptive. The fourth is that comparative advertising must not denigrate competitors. The fifth rule is that advocacy advertising must be distinguishable from factual information and the identity of the advertiser must be clearly stated. The sixth is that only verified testimonials and endorsements may be used. The seventh and eight rules regulate food and beverage advertising and environmental claims respectively. [95]

The Advertising Standards Authority runs an advertising complaints process under which anyone can make a complaint using their online complaints form available on their website. If a complaint is received, all parties

[87] 'About us' <https://www.asa.co.nz/about-us/> accessed 15 April 2021.
[88] ibid.
[89] ibid.
[90] ibid.
[91] 'Codes' <https://www.asa.co.nz/codes/> accessed 15 April 2021.
[92] Advertising Standards Code' <https://www.asa.co.nz/codes/codes/advertising-standards-code/.> accessed 16 April 2021.
[93] Advertising Standards Code' <https://www.asa.co.nz/codes/codes/advertising-standards-code/.> accessed 16 April 2021.
[94] ibid.
[95] Advertising Standards Code' <https://www.asa.co.nz/codes/codes/advertising-standards-code/.> accessed 16 April 2021.

associated with the specific advertisement must respond to the Advertising Standards Authority. The Advertising Standards Complaints Board is responsible for making decisions following complaints and responses by the parties. The Board consists of 9 members: five members being public members and 4 members belong to the advertising industry.[96] The decisions made may be appealed and if there are grounds for appeal, the appeal Board will re-consider the complaint. In case the Board agrees with the complainant, the advertiser may be asked to remove or amend the advertisement. In the situation that the Board finds that no rule of the *code* has been breached, then the Board may rule that there are no grounds to proceed. Sometimes, the Board may find that they lack the requisite jurisdiction to deal with the complaint as the Advertising Standards Authority deals only with advertisements targeted at New Zealand audiences, and any other advertisements will be out of its jurisdiction.[97]

Conclusion

New Zealand's government is actively working to carry all of its work online and ensure that its citizens benefit from it. Through the implementation of this process, it has sought to ensure inclusion and equal representation of all citizens as well. This country-specific report has strived to draw out the New Zealand-specific analysis in relation to the points put forward. In this regard, various aspects relating to privacy, personal data, information security, and intermediary regulation have been looked into. While there are many areas for the government to make changes to, New Zealand's initiatives in this regard is a step in the right direction.

[96] 'Complaints Board (ASCB) Members' <https://www.asa.co.nz/about-us/complaints-board-ascb-members/> accessed 17 April 2021.

[97] 'Advertising Standards Code' <http://www.asa.co.nz/wp-content/uploads/2019/03/Advertising-Standards-Code-2018.pdf> accessed 17 April 2021.

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 (SCMs) 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?
3. 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?
4. Should online platforms be immune from liability from third-party, user generated content [refer to intermediary liability laws]?
5. What should the parameters to define problematic user-generated content be?
6. Should online platforms moderate 'fake news', and if so, why?
7. 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.]
8. How does the global intermediary ecosystem shift from a post-hoc, harm-prevention lens to a proactive approach towards understanding and regulating technology?
9. Do the guidelines/policies of online platforms account for fallibility of the algorithm and the human content moderators, and if so, to what extent?
10. 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?
11. 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