**Legal Jurisdictions In A Digital Age: Challenges And Opportunities In Parliamentary Oversight Of Social Media Platforms**

**Rachel Tan**

Lecturer in Law (University of Waikato, New Zealand)

**Abstract**

This article explores the challenges and opportunities of legal jurisdictions in the digital age, focusing on parliamentary oversight of social media platforms. The internet's global nature has revolutionised communication, commerce, and social interactions, creating complex debates on law enforcement authority in the digital domain. Traditional jurisdiction concepts, tied to geography, are challenged by the internet's borderless nature, complicating the determination of applicable laws when content and actions span multiple countries.

Parliamentary oversight addresses these challenges by establishing clear legislative frameworks and fostering international cooperation. The Christchurch shootings in New Zealand highlighted the internet's role in distributing harmful content, underscoring the need for effective regulation. Similarly, the potential TikTok ban in the US demonstrates the complexities of addressing national security concerns, data privacy, and foreign influence through legislative action.

This article examines the Harvard Research Draft Convention on Jurisdiction with Respect to Crime and principles of sovereignty, comity, and non-intervention to highlight the evolving landscape of internet jurisdiction. It also emphasises the importance of balancing national laws with international standards to ensure fair and effective regulation. Ultimately, Parliamentary oversight can ensure that terms of service, data access requests, and content removal orders are transparent, fair, and consistent with both national and international legal frameworks.

**Introduction**

To understand the nature of legal jurisdictions in the digital age, we must first explore the traditional concept of jurisdiction. Traditional concept of jurisdictions link to geography and are essentially difficult to ascertain in the cyber sphere. The advent of the internet has resulted in a significant paradigm shift in the manner in which individuals communicate, engage in commercial activities, and participate in social interactions. The internet has sparked debates on how laws in the digital space can be enforced. The inherent global character of the internet poses a multifaceted difficulty when it comes to the implementation of rules and regulations across many countries and areas. The issue of jurisdiction holds significant importance due to the inherent characteristics of the cyber realm which has global reach by design.

The complexity of the internet’s impact on the conventional notion of jurisdiction can be distilled into two key issues.[[1]](#footnote-1) Firstly, there is the challenge posed by the Internet’s lack of a centralised authority.[[2]](#footnote-2) As an entity without ownership or control by any specific company or government, the Internet exists as a borderless realm.[[3]](#footnote-3) Consequently, when one is online, they inhabit a space that is simultaneously ubiquitous and devoid of a specific location.[[4]](#footnote-4)

Suppose I am in New Zealand, and Person A in the Netherlands posts something hateful about me on social media. Laws from New Zealand, the Netherlands, and possibly California (if the platform is based there) could apply. Additionally, if I’m a Singaporean citizen, Singaporean law might also be relevant. This highlights the complexity of jurisdiction in the digital age, where multiple countries' laws can be applicable regardless of physical geography. In addition to that scenario, it would also be worth considering the location of the *audience* of that post. My *friends* and *connections* on social media. This, therefore, demonstrates that determining countries is important. These countries will have their own scope of jurisdiction. The example further illustrates that geography is irrelevant when applied to the digital space.

In recent years, social media platforms have increasingly become tools not just for public engagement but also for malicious cyber activities. From coordinating cyberattacks to spreading disinformation and radicalising individuals, social media has been a conduit for both harmful behaviour and large-scale cyber threats. This connection emphasises the need for stringent regulation and parliamentary oversight, as the misuse of these platforms poses significant risks to national security and societal well-being.

On March 15, 2019, a remarkable display of aggression was observed by the global community. The accused individual, Brenton Tarrant, perpetrated a grievous offence that profoundly impacted the community of Christchurch. The individual in question was formally accused of committing the act of homicide against a total of 51 individuals, in addition to being confronted with an extra 40 allegations of engaging in acts of attempted murder. These charges are directly linked to the deeply distressing incidents that transpired at two mosques situated in Christchurch.[[5]](#footnote-5)

However, what rendered this calamity even more disconcerting was Tarrant's intention to disseminate his actions globally. The individual affixed a camera to their helmet, with the purpose of broadcasting their activities in real-time on several social media platforms, including Facebook.[[6]](#footnote-6) The live-streamed video footage would provide insight into the magnitude of his malicious intentions, so significantly influencing our understanding of the convergence of technology, legal systems, and acts of severe violence.

Brenton Tarrant live-streamed his attack on two mosques in Christchurch, New Zealand, broadcasting horrific acts of violence via social media. The Classification Office deemed the livestream objectionable under Section 3(1) of the Films, Videos, and Publications Classification Act (Classifications Act) due to its extreme violence, cruelty, and potential to incite further radicalisation.[[7]](#footnote-7) This case exemplifies the complexities of applying traditional legal frameworks to digital content, highlighting the urgent need for reform to address internet-related offences effectively. [[8]](#footnote-8)

The Classification Office also noted the use of extremist memes and cultural references in Tarrant's footage, including symbols tied to white supremacy and anti-immigrant sentiment. [[9]](#footnote-9) These references, along with his dehumanising portrayal of victims, further justified the classification of the content as objectionable under the FVPC Act, highlighting the dangerous influence such material could have in inciting further violence. [[10]](#footnote-10)

The Classification Office may decide upon examination and classification following section 23(2) of the Classifications Act. As a result of considering the aforementioned cultural references and with contemplation of section 3(4)(a)-(f) of the Classifications Act[[11]](#footnote-11), the Classifications Office deemed that the livestream footage contained extreme violence and extreme cruelty inflicted on the victims. Upon contemplating those considerations, the Classifications Office rationalised that it is in the public’s best interest that the footage is objectionable because:

“…

1. It would be traumatic for the relatives and friends of victims to view;
2. It could bring about re-victimisation for survivors if the video is made public and that strangers are viewing it too;
3. It could provide a negative neurological effect on children and young persons as the video is substantially shocking, disturbing, traumatizing to watch. Risk of psychological disturbance;
4. It can be used as a propaganda tool to recruit extremist especially those susceptible to being radicalised;
5. The video may serve as a form of ‘manual’ on the manner to conduct a mass murder;
6. If the video continues to being shared, the author that is the owner and creator of the video gets recognition and notoriety by way of violent means”[[12]](#footnote-12)

Usually, as with other criminal offences, the Courts will determine if a something is objectionable or not. For it to be deemed *objectionable*, a publication will meet the deliberation of the Classifications Office where the Chief Sensor makes the final judgement. With the Christchurch shooting, the courts looked at a manifesto which had been written and shared onto the internet.

The same effect was applied to Tarrant’s terrorist manifesto following the Christchurch shootings, which propagated extremist ideologies, such as white supremacy and anti-immigrant sentiment, under the guise of protecting white cultural identity. The manifesto included racist narratives that contributed to its classification as objectionable under New Zealand's Classifications Act. By disseminating such violent and hateful ideas, the manifesto became a dangerous tool for inciting further violence, making its prohibition crucial for preventing harm and deterring the spread of extremist ideologies.

The Classifications Act has often been reactionary, responding to events like the Christchurch shootings rather than proactively addressing the digital age’s challenges. This highlights the need for legislative reform. While the judiciary has had to creatively interpret the Act to encompass internet-related offences, such as classifying the terrorist manifesto as objectionable, parliamentary oversight is crucial in updating legal frameworks. This would ensure that laws effectively regulate harmful content across borders.

As part of the response to the recommendations by the Royal Commission of Inquiry into the attacks in Christchurch in 2019[[13]](#footnote-13), the Government at the time put forward the "Proposal against incitement of hatred and discrimination" (‘the Proposal’) by the Ministry of Justice. [[14]](#footnote-14) The premise behind these proposals was to address the root causes of extremism and foster social cohesion within the community as there are gaps in the current legislative framework. [[15]](#footnote-15) Additionally, alongside the proposed legislative reforms, careful consideration was given to The Treaty of Waitangi. This foundational document holds significant relevance in shaping incitement laws and safeguarding against discrimination, as outlined in both the Human Rights Act and the recommendations put forth in the Proposal. This is because Māori communities, in particular, face the harmful effects of hate speech and are currently protected under incitement legislation addressing 'race' or 'ethnic origin.'[[16]](#footnote-16) The concepts outlined in the Proposal aimed to strengthen protections for ethnic groups, including Māori, against hate speech.[[17]](#footnote-17) In addition, these enhanced protections will extend to Māori individuals facing discrimination based on other prohibited grounds, such as in the case of takatāpui.[[18]](#footnote-18) Regrettably, the ambitious Proposal outlined above was abandoned following the change in government. The then Labour administration lost the subsequent general elections, which means there is no continuity for this Proposal to progress into a Bill, as it does not align with the objectives or mandates of the current coalition government in 2024.

This case exemplifies the complexities of regulating digital content across borders. It underscores the challenges parliaments face in updating outdated legal frameworks like the FVPC Act to reflect the reality of internet-based offences. In the wake of incidents like the Christchurch attack, parliaments worldwide have recognised the need for tighter regulation of social media platforms. For instance, the New Zealand Parliamentary Service recently banned TikTok from parliamentary devices due to security risks, demonstrating the increasing role of parliaments in overseeing digital platforms.[[19]](#footnote-19)

**The Harvard Research Draft Convention on Jurisdiction with Respect to Crime (Harvard Draft)**

The global reach of digital platforms underscores the need for international cooperation on jurisdiction. The Harvard Research Draft Convention on Jurisdiction with Respect to Crime serves as a vital framework, especially in the digital age, guiding jurisdictional decisions to balance sovereignty with the global nature of the internet. Expert in Internet jurisdiction, Professor Dan J.B. Svantesson argues that jurisdiction is a relevant matter to the internet and that law enforcement would face challenges arising from both traditional crime and cybercrime if a state adopts a territoriality-centric approach to jurisdiction.[[20]](#footnote-20)

The Harvard Research Draft Convention on Jurisdiction with Respect to Crime, also known as the "Harvard Draft," was published in the American Journal of International Law in 1935, marking a significant advancement in international law.[[21]](#footnote-21) It is reasonable to assume that the framework that was proposed in the Harvard Draft has been the basis for the approach to jurisdiction in public international law ever since it was developed.[[22]](#footnote-22)

The most obvious reason why the Harvard Draft has had such an enormous influence is, of course, the fact that it represents a sterling research effort performed by top scholars, resulting in a convenient summary of a complex topic, which was published in a prestigious outlet at the right moment in time. This is why the Harvard Draft has had such an enormous influence in establishing jurisdiction.[[23]](#footnote-23)

The Territoriality principle holds immense significance, as highlighted in the Harvard Draft, where it is deemed of primary importance and essential in nature.[[24]](#footnote-24) Notably, applying this concept in today’s culture poses considerable challenges, particularly in the context of the internet, where its adaptation has proven to be high.[[25]](#footnote-25) The idea that it is difficult or perhaps impossible to identify the location of activities that take place online was a central theme in early discussions, further complicating the application to online realms.

Continued dialogue remains imperative, especially in the context of cloud computing. However, the ongoing debate has advanced to a critical juncture where the primary concern revolves around the extensive online activities that traverse state borders without establishing substantial, tangible connections to those specific states.[[26]](#footnote-26) This evolution of the conversation underscores the urgency of addressing the complex interplay between online activities and territorial jurisdictions.[[27]](#footnote-27) Svantesson posits that the ongoing discussions surrounding these issues serve as a potential catalyst, instigating a transformative shift in the way international law grapples with the multifaceted concept of jurisdiction.[[28]](#footnote-28) These debates unfold within a complex framework that encompasses not only the Harvard Draft principles but also intertwines additional elements such as (territorial) sovereignty, comity, and the obligation of non-interference. [[29]](#footnote-29) This intricate system operates within a recognised paradigm that exhibits shortcomings and inefficiencies, indicating a pressing need for comprehensive reform to reconcile these divergent components and effectively address the evolving challenges posed by modern global interactions and the digital landscape.[[30]](#footnote-30)

Furthermore, Svantesson emphasises the scarcity of approaches to the challenge of internet jurisdiction that cannot be both advocated for and contested in light of fundamental principles of public international law, encompassing (territorial) sovereignty, comity, non-intervention obligations, and the jurisdictional tenets proposed in the Harvard Draft.[[31]](#footnote-31)

The Harvard Draft delineates three fundamental tenets encapsulating the jurisdictional principles. These fundamental principles constrain the exercise of jurisdiction in the absence of binding international law obligations: firstly, establishing a substantial connection between the matter and the asserting state; secondly, the demonstrating of a legitimate interest by the asserting state in the matter; and thirdly, prioritising a delicate equilibrium between the state’s legitimate interests and those of other relevant entities.[[32]](#footnote-32) While this latter principle may not overtly manifest in the Harvard Draft as explicitly as the preceding two, its practical application becomes discernible through an examination of related principles, such as the protective principle, in real-world scenarios.[[33]](#footnote-33) The concerns regarding jurisdictional allegations are significantly influenced by the three core tenets outlined in the Harvard Draft. The pragmatic implementations of these principles, namely in the analysis of concepts such as the protective principle, provide valuable insights into the intricate complexity inherent in the field of international law.

The internet's borderless nature complicates legal jurisdiction, particularly when regulating platforms like Facebook and Google. An example is Facebook’s decision in 2021 to block Australian news organisations after the Australian government introduced a media law to ensure proper compensation for media content.[[34]](#footnote-34) This case underscores how global platforms challenge national jurisdiction when local laws affect international operations.

Censorship also presents a jurisdictional challenge. Historically focused on books, censorship now encompasses digital media like caricatures and computer games. For instance, the *Google Inc. v. Equustek Solutions Inc.[[35]](#footnote-35)* case in Canada demonstrates how censorship can affect international governance. In this case, Google was ordered to globally de-index websites that unlawfully sold intellectual property, raising jurisdictional questions about cross-border enforcement and the limits of local courts' influence over the global internet.[[36]](#footnote-36)

While censorship can be a tool for limiting harmful content, it also risks infringing on free speech and civil liberties. The balance between enforcing national laws and respecting international norms becomes particularly challenging in cyberspace, where different legal systems collide.

**Challenges of Legal Jurisdiction on social media**

Dealing with legal jurisdiction on the internet contains many problems. It is not as easy as it might seem at first. The thing is that in real life, when you want to sue somebody, you go to a court and file an application, and at some point, you get a legal decision according to which you are right, and the person you sued is guilty. But how do you do the same thing in cyberspace, where there are no territorial borders, where you are constantly moving from one country’s server to another’s, where the person you just had a fight with online lives on the other side of the globe?

The global reach of online activities blurs the lines of geographical confinement, sparking intricate debates over which legal system holds sway over digital content and activities spanning multiple nations. Jurisdiction can have a legislative approach whereby a state has enforcement powers at a specific level. The terms *jurisdiction* and *power* represent separate ideas.[[37]](#footnote-37) In the Laws of New Zealand[[38]](#footnote-38), jurisdiction is defined as ‘the authority possessed by a Court to adjudicate on issues brought before it or to recognise matters formally submitted for its decision.’[[39]](#footnote-39) This interplay between the traditional confines of legal authority and the borderless nature of the internet engenders a myriad of complexities, presenting a pressing need for comprehensive solutions in navigating jurisdictional intricacies online. For example, a website that is hosted in one country may be accessible from another country where the content is illegal or violates local laws. In such cases, the question arises as to which country's laws should apply. Similarly, a person who engages in illegal activity online may be located in a different country than the victims of that activity, making it difficult to determine which country's legal system should have jurisdiction over the case.

Enforcing laws across digital borders present challenges. A court in one country may issue a ruling, but enforcing it across borders—where content or data may be located in different countries—complicates matters. This issue highlights the growing need for coordinated international legal frameworks.

The method in which we communicate with one another, run our businesses, and exchange information has been profoundly altered as a direct result of the proliferation of the internet. On the other hand, due to its worldwide nature, the internet poses a number of difficulties for the exercise of legal authority. At this juncture, it is important to consider the question, *what are the difficulties associated in exercising legal authority over the internet?*

The adoption of a territoriality-centric approach to jurisdiction by a state would pose dual challenges for law enforcement, encompassing both traditional and cyber crime scenarios.[[40]](#footnote-40) For a deeper understanding to territoriality, the “Lotus”[[41]](#footnote-41) case “Harvard Draft Convention on Jurisdiction with Respect to Crime”[[42]](#footnote-42) will be important as a source of reference[[43]](#footnote-43). The current paradigm is characterized by a territoriality mentality[[44]](#footnote-44).

With constant technological innovation over time comes the complexities of regulating both legitimate and criminal operations over social media. The evolution of crime has frequently been outpaced by the development of legislation and law-enforcement capabilities, resulting in disparities or asymmetries between jurisdictions[[45]](#footnote-45). Technology has also modified some of the core notions on which general criminal law and law are based primarily on areas such as privacy, property and jurisdiction, as they become interwoven into the global network[[46]](#footnote-46). With this, customary and traditional concepts of criminal jurisdiction and the use of the internet as a means of communication have faced their challenges because of the internet’s global nature[[47]](#footnote-47).

Even if, for a moment, we set aside the sheer number of online publishers that could potentially face prosecution for sharing illegal or posting harmful content online (a task that requires a lot of police and prosecutor resources), the transient nature of online publishers, operating across various countries, presents a significant legal challenge.[[48]](#footnote-48)

**Jurisdiction in Cyberspace**

Regarding jurisdiction, the focus lies on the sovereignty of nation-states. It is the state’s power to manage and govern its own territory and people. This sets the nature and limits of their jurisdiction.

For clarity, it is essential to comprehend the various jurisdiction-related scenarios. This understanding establishes the context for discussions and facilitates progress in this field. The term jurisdiction is particularly significant in three scenarios that raise substantial concerns for internet intermediaries.[[49]](#footnote-49)  These scenarios are as follows:

***A Community Guidelines or Terms of Service***

The legality of the **terms of service** that internet intermediaries generally impose on their end-users frequently includes crucial clauses addressing the applicable legislation and jurisdiction.[[50]](#footnote-50) Specifically, in the so-called choice-of-forum and choice-of-law agreements, significant and contentious legal issues arise at the intersection of private international law and internet intermediaries' practices.[[51]](#footnote-51) In context of online hate speech, this involves the examination of the legality of the terms of service that the social media platform typically imposes on its users. Most often, these terms would include such clauses addressing applicable legislation and jurisdiction. These agreements become crucial when legal issues emerge regarding the practices of these platforms and their alignment with internal law.

A choice-of-law clause determines the applicable law in a lawsuit, while a choice-of-forum clause designates the court for dispute resolution. These clauses are commonly found in the terms of services, although studies repeatedly show users rarely read or fully understand these agreements, often agreeing without complete awareness; such as click-wrap or browse wrap agreements. For instance, by engaging on a social media platform that offers its terms of service through a link on the app or website, one might be seen as giving implied consent, even if they have not directly read it, accessed, or explicitly agreed to those terms.[[52]](#footnote-52)

In a German case[[53]](#footnote-53), two of its German citizens contested Facebook’s decision to remove their posts and temporarily disable their accounts in a court dispute.[[54]](#footnote-54) In their posts, the first Facebook user disparaged immigrants and criticised the German Reich Citizens. [[55]](#footnote-55) The second Facebook user posted a video implying that immigrants would never integrate into Germany.[[56]](#footnote-56) The actions by the two Facebook users contravened the social media platform’s hate speech Community Guidelines as of 19 April 2018.[[57]](#footnote-57) As a result, the individuals sued Facebook, arguing that Facebook had violated their right to freedom of expression under German law.[[58]](#footnote-58) In addition, they contended that its terms of service were unfair and disadvantageous to users. [[59]](#footnote-59)

The court in first instance, The Regional Court in Nuremberg and subsequently, The Higher Regional Court Nuremberg initially ruled in favour of Facebook. It held that the social media platform could enforce higher communication standards beyond legal requirements.[[60]](#footnote-60) The courts did this by balancing the users’ freedom of expression against Facebook’s interest in maintain a safe online environment.

This matter was finally brought before the Federal Court of Justice in Germany, where an assessment was conducted to determine the legality of Facebook’s actions. [[61]](#footnote-61) The Federal Court of Justice’s determination stipulated that although private corporations (such as Facebook) are not directly obliged by the freedom of expression legislation laws like state entities, they are subject to constitutional issues within the realm of private legal relationships.[[62]](#footnote-62) In addition, the Court recognised the user’s rights to freedom of expression, yet at the same time acknowledged Facebook’s rights to manage and regulate content on its platform to ensure a respectful online environment. [[63]](#footnote-63) According to the Court, Facebook possessed the ability to establish regulations governing communications and it has the authority to remove any content that fails to adhere to these rules. Nevertheless, this emphasised the necessity for well-defined and comprehensive rules and protocols pertaining to content moderation.

The Court then ruled that the terms of service therefore was inadequate and lacked procedural safeguards thereby disadvantaging its users. [[64]](#footnote-64) Its recommendation was to require Facebook to inform users about takedowns or content removals and account blocking, allowing users to respond before any action. It stressed on maintaining a reasonable content moderation process while balancing the user’s rights. The Court, therefore, invalidated parts of Facebook’s terms of service. Specifically, it found that Facebook lacked the authority to remove its users’ posts or block their accounts based on those terms. [[65]](#footnote-65) The Court issued a directive to have Facebook reinstate the deleted posts.

##### ***Requesting access to user data***

The second scenario concerns circumstances where law enforcement organisations ask internet intermediaries for access to user data. Such cases raise important jurisdictional questions, not only when the requesting law enforcement agency and the internet intermediary are based in different nations, but they may also do so, as was demonstrated in the well-known Microsoft Warrant case when the requested data is stored outside of the nation in which both the law enforcement agency and the internet intermediary are based.[[66]](#footnote-66)

##### ***Geographic area***

The third illustration concerns the issue of the geographic area where an online intermediary is needed to take down, remove, block, delist, de-index, or de-reference content.[[67]](#footnote-67) An example of where geographical area becomes a challenge and the measures used in this instance will be illustrated in the case of *Google Inc. v. Equustek Solutions Inc.*[[68]](#footnote-68)

When it comes to matters of international law, the majority of states develop their own policies and protocols. Private international law is the specific subfield of the legal system that pertains to territorial disputes. The norms of private international law that are applicable in many states provide for jurisdictional and legislative claims to be made over any website that may be viewed in its territory with regards to a wide variety of different types of legal issues. These claims can be made in relation to any website, regardless of where the website is hosted.

The concept of territorial jurisdiction stems from the principles of sovereign equality, deference, and non-interference by one state in the internal affairs of another and the direction that each state has exclusive sovereignty over its laws and their application to events in its territory[[69]](#footnote-69). How cybercrime was treated in the beginning is said to be akin to the concept of *terra nullius,* that is, in the cyber sphere, whereby the notion of cyberspace was as if it were a physical location and a new territory. This notion led to initial misconceptions about its governance and regulation.[[70]](#footnote-70)

**Legal Frameworks and Collaborative Initiatives**

In the European Union, the Framework Decision prescribes a set of criteria to determine when a crime should be considered as having been committed within the jurisdiction of a Member State. This is the case if an act, or part of it, which is relevant to establishing the nature of the crime or the identity of the perpetrator, takes place within the territory of the Member State, but also in specific other situations concerning residents and bodies incorporated under national law.[[71]](#footnote-71) Where offences are committed using an information system, the Member State would have to take the necessary steps to ensure that the offence was physically conducted in its territory – regardless of whether the material in question is hosted on a system in its territory or not.[[72]](#footnote-72) This therefore demonstrates the idea that jurisdiction might be based on the physical location of the criminal act rather than the location of the digital information or systems used in committing the offense.

*Initiatives on online hate speech*

In 2016, the European Commission and leading IT companies jointly announced and ratified a Code of Conduct.[[73]](#footnote-73) This Code of conduct sets out a series of commitments aimed at fostering collaboration between the European Commission and major tech entities such as Facebook, YouTube, Twitter and Microsoft.[[74]](#footnote-74)

The primary commitments outlined in the Code of Conduct entail a proactive stance by IT Companies against online hate speech. [[75]](#footnote-75) This involves implementing robust and transparent processes within each company, particularly in the diligent review of reported instances concerning hate speech. This includes a clear and effective process established by every IT Company, ensuring prompt assessment for the removal of contentious content.[[76]](#footnote-76) Such procedures are defined within respective Rule and Community Guidelines, explicitly prohibiting content that incites violence or promotes hateful conduct. In the event of a breach of these guidelines by an individual or entity, a notification is directed to IT companies for review and potential content removal, adhering to the strict 24-hour review timeframe.[[77]](#footnote-77)

IT companies are poised to play a critical educational role by enlightening their users about prohibited content in line with their Community Guidelines. They aim to empower users with knowledge on how to report instances of online hate speech or prohibited content. [[78]](#footnote-78)Moreover, there's a strong recommendation for IT Companies to establish swift and effective communication channels with authorities from Member States. This entails seamless procedures for notifying and promptly removing or disabling access to online hate speech content. [[79]](#footnote-79)

To facilitate this exchange of information, the Code of Conduct suggests utilising national contact points jointly appointed by both IT companies and Member States. This collaborative approach seeks to acquaint law enforcement agencies and Member States with effective methodologies for identifying and reporting instances of online hate speech.[[80]](#footnote-80)

*Initiatives on cyber threats*

Cyber threats are happening more and more, which points to the need for improved national resilience in cyber security. A prime example of this necessity is the May 2021 cyber attack on the Waikato District Health Board, which dismantled services and treatments for an extended period, demonstrating the need for well-thought-out cyber security strategies.[[81]](#footnote-81)

In 2023, an essential document was provided to the incoming Minister for the Digital Economy and Communications. Titled "Incoming Minister Briefing," the document prioritizes responsibilities for the Minister related to the highly complex and urgent matter of cyber security policy. [[82]](#footnote-82) At the top of the list, the Minister must supervise the continuous enhancement and coordination of New Zealand's Cyber Security Strategy and its associated initiatives in an effort to keep the country’s cyber security not only coordinated but also flexible and adaptable to a rapidly changing threat environment.

Policy development is another critical facet, especially as it relates to the cyber resilience of New Zealand's individuals, businesses, and providers of essential infrastructure.[[83]](#footnote-83) There is also a considerable emphasis on addressing the national security threats associated with digital technologies—especially new and emerging tech and applications. [[84]](#footnote-84) Meeting the challenges these pose requires not just policy development at a high level but also engagement with and understanding of the technological base and pace that policy has to upkeep in order to remain relevant and to serve the public good.

When cybersecurity incidents occur, it's crucial to establish appropriate policy responses, which include publicly attributing the incidents after consulting relevant ministers to maintain transparency and accountability. Additionally, addressing national security risks posed by cybercrime requires well-coordinated and targeted policy efforts to ensure a comprehensive response. This includes working with global partners and consulting the Minister of Foreign Affairs to ensure New Zealand's cybersecurity strategies are aligned with international standards and practices.[[85]](#footnote-85)

The 2022/2023 Cyber Threat Report by the National Cyber Security Centre (NCSC) outlines key challenges for New Zealand in cyberspace.[[86]](#footnote-86) The country faces a more complex threat environment, with cybercriminals using increasingly sophisticated techniques that challenge traditional defences. Emerging technologies, like generative AI, add new risks to privacy and security. Notably, financially motivated cyber activities have, for the first time, surpassed state-sponsored threats, posing a greater impact on New Zealand’s overall security and well-being.[[87]](#footnote-87)

Protecting critical infrastructure from cyber threats remains a priority, with efforts to enhance the resilience of essential services and mitigate potential disruptions.[[88]](#footnote-88) Ransomware and extortion activities have a significant presence, with incidents causing substantial recovery efforts and financial impact. The rapid adoption of technologies such as AI requires careful governance to control privacy and security risks associated with their use.

To address growing cyber threats, New Zealand relies on international cooperation for intelligence sharing, including efforts involving parliamentary oversight of digital platforms like social media. [[89]](#footnote-89) Social media can both amplify cybersecurity risks and serve as a tool for public engagement. Parliament's role in regulating and overseeing these platforms is crucial in mitigating risks while ensuring transparency. Strengthening New Zealand's cybersecurity workforce and fostering international policy collaboration aligns with parliament's goals to protect the nation’s digital infrastructure and national security interests. Recent developments highlight Parliament's growing role in managing digital risks, as demonstrated by the New Zealand Parliamentary Service's decision to ban TikTok from official devices due to concerns over data security.[[90]](#footnote-90) This exemplifies the critical oversight responsibilities of legislative bodies in regulating digital platforms to safeguard national security while balancing public engagement through social media.

**Conclusion**

Legal jurisdiction on the internet is a complex issue that raises a number of challenges for legal systems around the world. The global nature of the internet means that activities may take place in different countries and be subject to different laws and regulations. However, different legal systems have developed a range of approaches to address this issue, from territorial approaches to more flexible frameworks that take into account the global nature of the internet.

The internet is commonly referred to as the ‘Wild West’ due to the challenges in enforcing laws.[[91]](#footnote-91) The enforcement of court rulings across borders, such as those pertaining to Google, fosters a disregard for legal principles on the internet, leaving internet companies in the challenging predicament of deciding which laws and court orders to adhere to. Disregarding foreign court rulings undermines legal certainty online, promoting cross-border litigation and a worldwide perspective on domestic laws.

In conclusion, the challenges of legal jurisdiction in the digital age, especially concerning social media platforms, demand urgent attention from both national governments and international bodies. The borderless nature of the internet, exemplified by the Christchurch attack, highlights the critical need for updated legal frameworks that address internet-related offences. Parliamentary oversight must evolve to regulate digital platforms effectively, balancing national security and freedom of expression.

This will require robust international collaboration, consistent policy reform, and the strengthening of cybersecurity to protect citizens and critical infrastructure. Only by implementing these comprehensive measures can parliaments safeguard their digital jurisdictions and maintain public trust in the evolving online world.

This article emphasises the importance of continuous adaptation and reform to meet the challenges posed by the global digital landscape. The role of social media, which can both enhance public engagement and introduce cybersecurity risks, must be carefully regulated through effective legislation and parliamentary oversight.

1. Nehaluddin Ahmad and Norulaziemah Zulkiffle, ‘Jurisdiction Issues in Cyberspace: An Overview in Respect of Brunei and Malaysia Compared to The United States' System’ *Journal of Southeast Asian Research Article* 2022 [↑](#footnote-ref-1)
2. Ahmad and Zulkiffle, *‘Jurisdiction Issues in Cyberspace: An Overview in Respect of Brunei and Malaysia Compared to The United States' System’* [↑](#footnote-ref-2)
3. Ahmad and Zulkiffle, *‘Jurisdiction Issues in Cyberspace: An Overview in Respect of Brunei and Malaysia Compared to The United States' System’* [↑](#footnote-ref-3)
4. Ahmad and Zulkiffle, *‘Jurisdiction Issues in Cyberspace: An Overview in Respect of Brunei and Malaysia Compared to The United States' System’* [↑](#footnote-ref-4)
5. BBC, ‘Christchurch shootings: 49 dead in New Zealand mosque attacks’. Accessed at: https://www.bbc.com/news/world-asia-47578798 [↑](#footnote-ref-5)
6. *R v Tarrant* [2020] NZHC 2192. [↑](#footnote-ref-6)
7. *Film, Video, and Publications Classifications Act 1993* (NZ), s3(1) [↑](#footnote-ref-7)
8. The Classification Office - Te Mana Whakaatu, ‘Christchurch Mosque Attack Livestream’, Accessed at: [<https://www.classificationoffice.govt.nz/news/featured-classification-decisions/christchurch-mosque-attack-livestream/>.](%3Chttps%3A//www.classificationoffice.govt.nz/news/featured-classification-decisions/christchurch-mosque-attack-livestream/%3E.) [↑](#footnote-ref-8)
9. The Classification Office - Te Mana Whakaatu, ‘Christchurch Mosque Attack Livestream’. [↑](#footnote-ref-9)
10. The Classification Office - Te Mana Whakaatu, ‘Christchurch Mosque Attack Livestream’. [↑](#footnote-ref-10)
11. The Classification Office - Te Mana Whakaatu, ‘Christchurch Mosque Attack Livestream’. [↑](#footnote-ref-11)
12. The Classification Office - Te Mana Whakaatu, ‘Christchurch Mosque Attack Livestream’. [↑](#footnote-ref-12)
13. Royal Commission of Inquiry Into The Terrorist Attack On Christchurch Mosques On 15 March 2019 'Questions about the Royal Commission of Inquiry', Accessed at: <https://christchurchattack.royalcommission.nz/about-the-inquiry/questions-about-the-royal-commission-of-inquiry/>. [↑](#footnote-ref-13)
14. Ministry of Justice, 'Proposal against incitement of hatred and discrimination', Accessed at: <https://www.justice.govt.nz/assets/Documents/Publications/Incitement-Discussion-Document.pdf>. [↑](#footnote-ref-14)
15. Ministry of Justice, 'Proposal against incitement of hatred and discrimination’. [↑](#footnote-ref-15)
16. Ministry of Justice, 'Proposal against incitement of hatred and discrimination’. [↑](#footnote-ref-16)
17. Ministry of Justice, 'Proposal against incitement of hatred and discrimination’. [↑](#footnote-ref-17)
18. Te Aka Māori Dictionary, 'Takatāpui' Accessed at: <https://maoridictionary.co.nz/search?idiom=&phrase=&proverb=&loan=&histLoanWords=&keywords=takatapui>. *Takatāpui* is defined as (noun) lesbian, gay, homosexual, gay men and women. [↑](#footnote-ref-18)
19. Rafael Gonzalez-Montero, ‘Media statement: TikTok on Parliamentary Service devices’, *New Zealand Parliament Pāremata Aotearoa*, 17 March 2023, Accessed at https://www.parliament.nz/en/footer/about-us/parliamentary-service/parliamentary-service-media-releases/media-statement-tiktok-on-parliamentary-service-devices/ [↑](#footnote-ref-19)
20. Dan Jerker B. Svantesson "Lagom jurisdiction” – What drinking etiquette can teach us about internet jurisdiction and Google France" 2018 Masaryk University Journal of Law and Technology 29 at 33. [↑](#footnote-ref-20)
21. Dan Jerker B. Svantesson, 'A New Jurisprudential Framework For Jurisdiction: Beyond The Harvard Draft'. *AJIL Unbound* 109 2015, p.69. [↑](#footnote-ref-21)
22. Svantesson, 'A New Jurisprudential Framework For Jurisdiction: Beyond The Harvard Draft'. AJIL Unbound 109 2015, p.73. [↑](#footnote-ref-22)
23. Svantesson, 'A New Jurisprudential Framework For Jurisdiction: Beyond The Harvard Draft'. AJIL Unbound 109 2015, p.71. [↑](#footnote-ref-23)
24. Svantesson, 'A New Jurisprudential Framework For Jurisdiction: Beyond The Harvard Draft'. AJIL Unbound 109 2015, p.73. [↑](#footnote-ref-24)
25. Svantesson, 'A New Jurisprudential Framework For Jurisdiction: Beyond The Harvard Draft'. AJIL Unbound 109 2015, p.73. [↑](#footnote-ref-25)
26. Svantesson, 'A New Jurisprudential Framework For Jurisdiction: Beyond The Harvard Draft'. AJIL Unbound 109 2015, p.69. [↑](#footnote-ref-26)
27. Svantesson, 'A New Jurisprudential Framework For Jurisdiction: Beyond The Harvard Draft'. AJIL Unbound 109 2015, p.69. [↑](#footnote-ref-27)
28. Dan Jerker B. Svantesson, *'A New Jurisprudential Framework for Jurisdiction'* Oxford: Oxford University Press, 2017. p.71. [↑](#footnote-ref-28)
29. Dan Jerker B. Svantesson, *'A New Jurisprudential Framework for Jurisdiction'* Oxford: Oxford University Press, 2017. P. 69. [↑](#footnote-ref-29)
30. Dan Jerker B. Svantesson, *'A New Jurisprudential Framework for Jurisdiction'* Oxford: Oxford University Press, 2017. p 72. [↑](#footnote-ref-30)
31. Dan Jerker B. Svantesson, *'A New Jurisprudential Framework for Jurisdiction'* Oxford: Oxford University Press, 2017. p 58. [↑](#footnote-ref-31)
32. Dan Jerker B. Svantesson, *'A New Jurisprudential Framework for Jurisdiction'* Oxford: Oxford University Press, 2017. P.69. [↑](#footnote-ref-32)
33. Dan Jerker B. Svantesson, *'A New Jurisprudential Framework for Jurisdiction'* Oxford: Oxford University Press, 2017. P.69. [↑](#footnote-ref-33)
34. Amanda Meade, ‘Australia is making Google and Facebook pay for news: what difference will the code make?’,  *The Guardian*, Accessed at: https://www.theguardian.com/media/2020/dec/09/australia-is-making-google-and-facebook-pay-for-news-what-difference-will-the-code-make [↑](#footnote-ref-34)
35. *Google Inc. v. Equustek Solutions Inc*. 2001 [2017] 1 SCR 824. [↑](#footnote-ref-35)
36. *Google Inc. v. Equustek Solutions Inc.* 2001 [2017] 1 SCR 824 at [2]. [↑](#footnote-ref-36)
37. Rosara Joseph, 'Inherent jurisdiction and inherent powers in New Zealand' *Canterbury Law Review* 220 2005, p. 13 [↑](#footnote-ref-37)
38. Joseph, 'Inherent jurisdiction and inherent powers in New Zealand' *Canterbury Law Review* 220 2005, p. 1. [↑](#footnote-ref-38)
39. Joseph, 'Inherent jurisdiction and inherent powers in New Zealand' *Canterbury Law Review* 220 2005, p. 1. [↑](#footnote-ref-39)
40. Dan Jerker B. Svantesson, 'Lagom jurisdiction – What drinking etiquette can teach us about internet jurisdiction and Google France' *Masaryk University Journal of Law and Technology* 29 2018 p.33.

at 33. [↑](#footnote-ref-40)
41. SS ‘Lotus” (France v Turkey) (1927) PCIJ Series A, No 10. [↑](#footnote-ref-41)
42. The American Journal of International Law “Harvard Draft Convention on Jurisdiction with Respect to Crime” 1935, Vol. 29, Supplement: Research in International Law 439. [↑](#footnote-ref-42)
43. Martina Mantovani, 'Jurisdiction, Conflict of Laws and Data Protection in Cyberspace' Accessed at: <https://conflictoflaws.net/2017/jurisdiction-conflict-of-laws-and-data-protection-in-cyberspace/>. [↑](#footnote-ref-43)
44. Dan Jerker B. Svantesson,'Jurisdictional issues and the internet – a brief overview 2.0' *Computer Law & Security Review* 34(715), 2018,p. 722. [↑](#footnote-ref-44)
45. Neil Boister and Robert J. Currie, '*Routledge Handbook of Transnational Criminal Law* Oxford: Routledge, London, 2014 p. 379. [↑](#footnote-ref-45)
46. Boister and Currie, '*Routledge Handbook of Transnational Criminal Law* Oxford: Routledge, London, 2014 [↑](#footnote-ref-46)
47. Boister and Currie, '*Routledge Handbook of Transnational Criminal Law* Oxford: Routledge, London, 2014 [↑](#footnote-ref-47)
48. Peter Coe "The Draft Online Safety Bill and the regulation of online harms and hate speech: have we opened Pandora’s Box?" (paper presented to BACL Annual Webinar: The Regulation of Hate Speech Online and Its Enforcement in a Comparative Perspective, London, 31 August 2021). [↑](#footnote-ref-48)
49. Dan Jerker B. Svantesson, *Internet Jurisdiction And Intermediary Liability*. Oxford: Oxford University Press, Oxford 2020 p. 488. [↑](#footnote-ref-49)
50. Svantesson, *Internet Jurisdiction And Intermediary Liability*. Oxford: Oxford University Press, Oxford 2020 p. 488 [↑](#footnote-ref-50)
51. Svantesson, *Internet Jurisdiction And Intermediary Liability*. Oxford: Oxford University Press, Oxford 2020 p. 488 [↑](#footnote-ref-51)
52. Jonathan A. Obar and Anne Oeldorf-Hirsch, 'The Clickwrap: A Political Economic Mechanism for Manufacturing Consent on Social Media'. *Social Media + Society* 4 2018, p. 3. [↑](#footnote-ref-52)
53. Bundesgerichtshof [BGH] [Federal Court of Justice] Jul. 29, 2021, 154 Entscheidungen des Bundesgerichtshofes in Zivilsachen [BGHZ] 370, 371 (Ger.). [↑](#footnote-ref-53)
54. Columbia Global Freedom of Expression, 'The Case on Facebook’s Terms of Service' Accessed at: <https://globalfreedomofexpression.columbia.edu/cases/the-case-on-facebooks-terms-of-service/>. [↑](#footnote-ref-54)
55. Columbia Global Freedom of Expression, 'The Case on Facebook’s Terms of Service' [↑](#footnote-ref-55)
56. Columbia Global Freedom of Expression, 'The Case on Facebook’s Terms of Service' [↑](#footnote-ref-56)
57. Columbia Global Freedom of Expression, 'The Case on Facebook’s Terms of Service' [↑](#footnote-ref-57)
58. Columbia Global Freedom of Expression, 'The Case on Facebook’s Terms of Service' & art. 5 (1) German Basic Law (Grundgesetz, GG) [↑](#footnote-ref-58)
59. Columbia Global Freedom of Expression, 'The Case on Facebook’s Terms of Service' [↑](#footnote-ref-59)
60. Columbia Global Freedom of Expression, 'The Case on Facebook’s Terms of Service' [↑](#footnote-ref-60)
61. Columbia Global Freedom of Expression, 'The Case on Facebook’s Terms of Service' [↑](#footnote-ref-61)
62. Columbia Global Freedom of Expression, 'The Case on Facebook’s Terms of Service' [↑](#footnote-ref-62)
63. Columbia Global Freedom of Expression, 'The Case on Facebook’s Terms of Service' [↑](#footnote-ref-63)
64. Columbia Global Freedom of Expression, 'The Case on Facebook’s Terms of Service' [↑](#footnote-ref-64)
65. Columbia Global Freedom of Expression, 'The Case on Facebook’s Terms of Service' [↑](#footnote-ref-65)
66. Columbia Global Freedom of Expression, 'The Case on Facebook’s Terms of Service' [↑](#footnote-ref-66)
67. Columbia Global Freedom of Expression, 'The Case on Facebook’s Terms of Service' [↑](#footnote-ref-67)
68. Michael Geist, *‘The Equustek Effect: A Canadian Perspective on Global Takedown Orders In The Age Of The Internet’* Oxford: Oxford University Press, 2020 p. 710. [↑](#footnote-ref-68)
69. Boister and Currie, '*Routledge Handbook of Transnational Criminal Law* Oxford: Routledge, London, 2014 [↑](#footnote-ref-69)
70. David Livingstone Paul Cornish, Dave Clemente and Claire Yorke, ‘Cyber Security

and the UK’s Critical National Infrastructure (A Chatham House Report, September 2011) Accessed at: https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r0911cyber.pdf [↑](#footnote-ref-70)
71. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') 2000 OJ L/178. [↑](#footnote-ref-71)
72. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') 2000 OJ L/178, above, n 897, art. 9 (2) (a) [↑](#footnote-ref-72)
73. European Commission, 'European Commission and IT Companies announce Code of Conduct on Illegal Online Hate Speech' Accessed at: https://ec.europa.eu/commission/presscorner/detail/en/IP\_16\_1937>. [↑](#footnote-ref-73)
74. European Commission, *'European Commission and IT Companies announce Code of Conduct on Illegal Online Hate Speech'*  [↑](#footnote-ref-74)
75. European Commission, *'European Commission and IT Companies announce Code of Conduct on Illegal Online Hate Speech'*  [↑](#footnote-ref-75)
76. European Commission, 'The Code of conduct on countering illegal hate speech online' Accessed at: <https://ec.europa.eu/commission/presscorner/detail/en/qanda\_20\_1135>. [↑](#footnote-ref-76)
77. European Commission, *'The Code of conduct on countering illegal hate speech online'.* [↑](#footnote-ref-77)
78. European Commission, *'The Code of conduct on countering illegal hate speech online'.* [↑](#footnote-ref-78)
79. European Commission, *'The Code of conduct on countering illegal hate speech online'.* [↑](#footnote-ref-79)
80. European Commission, *'The Code of conduct on countering illegal hate speech online'.* [↑](#footnote-ref-80)
81. INPHYSEC, New Zealand, *Waikato District Health Board (WDHB) Incident Response Analysis,* 2 September 2022, p.7 [↑](#footnote-ref-81)
82. Department of the Prime Minister and Cabinet -Te Tari O Te Pirimia Me Te Komiti Matua (31 January 2023), ‘*Briefing to the Incoming Minister for the Digital Economy and Communications’*, Accessed at: https://www.beehive.govt.nz/sites/default/files/2023-03/BIM%20-%20Minister%20for%20the%20Digital%20Economy%20and%20Communications%20-%20DPMC.pdf [↑](#footnote-ref-82)
83. Department of the Prime Minister and Cabinet -Te Tari O Te Pirimia Me Te Komiti Matua (31 January 2023), *‘Briefing to the Incoming Minister for the Digital Economy and Communications’* [↑](#footnote-ref-83)
84. Department of the Prime Minister and Cabinet -Te Tari O Te Pirimia Me Te Komiti Matua (31 January 2023), *‘Briefing to the Incoming Minister for the Digital Economy and Communications’* [↑](#footnote-ref-84)
85. Department of the Prime Minister and Cabinet -Te Tari O Te Pirimia Me Te Komiti Matua (31 January 2023), *‘Briefing to the Incoming Minister for the Digital Economy and Communications’* [↑](#footnote-ref-85)
86. Government Communications Security Bureau Te Tira Tiaki, ‘Cyber Threat Report 2022/2023’ Accessed at: https://www.ncsc.govt.nz/resources/ncsc-annual-cyber-threat-reports?url=resources%2Fncsc-annual-cyber-threat-reports%2F [↑](#footnote-ref-86)
87. Government Communications Security Bureau Te Tira Tiaki, ‘Cyber Threat Report 2022/2023’, p. 10 [↑](#footnote-ref-87)
88. Government Communications Security Bureau Te Tira Tiaki, ‘Cyber Threat Report 2022/2023’, p. 13 [↑](#footnote-ref-88)
89. Government Communications Security Bureau Te Tira Tiaki, ‘Cyber Threat Report 2022/2023’, p. 18 [↑](#footnote-ref-89)
90. Radio New Zealand. ‘Parliamentary Service bans TikTok on its devices’, Accessed at: https://www.rnz.co.nz/news/political/486167/parliamentary-service-bans-tiktok-on-its-devices [↑](#footnote-ref-90)
91. Michael Geist, *‘The Equustek Effect: A Canadian Perspective on Global Takedown Orders In The Age Of The Internet’* Oxford: Oxford University Press, 2020 p. 725. [↑](#footnote-ref-91)