DEPARTMENT OF THE PRIME MINISTER AND CABINET
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

Aide-Memoire

THE NORMS OF RESPONSIBLE STATE BEHAVIOUR IN CYBERSPACE

To	Rt Hon Jacinda Ardern, Prime Minister and Minister for National Security and Intelligence	**Report No**	2021/NSP/131
From	National Cyber Policy Office, Department of the Prime Minister and Cabinet	**Date**	29/06/2021

Purpose

1. You have requested a briefing on the norms of responsible state behaviour in cyberspace. This briefing outlines those norms and their development, as well as situating them in the broader "framework" of responsible state behaviour online. It also outlines trends and challenges, including where malicious cyber activity falls into a grey area with respect to the normative framework.

Background

2. Malicious actors are increasingly adaptive and strategic, conducting cyber activity below a threshold that allows them to achieve gains without risking outright conflict. There have been growing efforts over the past decade to articulate and develop "rules of the road" for cyberspace to better regulate how states (in particular) behave.[1]

3. In order to address this, a "Framework of Responsible State Behaviour in Cyberspace" has emerged from a number of different UN processes over the past decade.[2] This Framework has been endorsed by the UN General Assembly, most recently in April 2021. It is based on four pillars:

   - **International law**: all UN members agree that international law applies to states' conduct in cyberspace. Exactly how it applies remains contentious: for instance there is no agreement on how, or at what threshold cyber attacks impact state sovereignty and non-interference; what kind of cyber attack might constitute a "use of force" forbidden by Article 2.4 of the UN Charter; and whether or when Article 51, which defines the right of self-defence, would be triggered.[3]

[1] Individual criminal behaviour is not explicitly captured by these efforts because individuals cannot be held to international legal and normative frameworks.
[2] The two key processes through which this framework has developed are the *UN Group of Governmental Experts on Developments in the Field of Information and Communication Technologies in the Context of International Security* (GGE), and the *Open-Ended Working Group on Information and Communication Technology Developments in the Context of International Security* (OEWG).
[3] States have sought to clarify their positions on how international law applies in cyberspace through the publication of national position statements. New Zealand issued a national position statement in December 2020.

- Non legally-binding **norms of responsible state behaviour online**: there are 11 norms agreed in the UN context that are aimed at setting clear expectations of what states should and should not do in cyberspace during peacetime (see details below). Though voluntary, norms contribute to stability and security by building shared expectations of what constitutes acceptable and unacceptable behaviour in cyberspace.

- **Confidence-building measures**: initiatives which are aimed at supporting transparency, predictability, and stability in cyberspace. These might include initiatives which enhance states' mutual threat perceptions, clarify cyber capabilities, and explain respective structures or processes for crisis response.

- **Capacity-building measures**: aimed to help ensure that all states can lower the risks of increased connectivity, while still benefiting from it. This might include initiatives that assist states in implementing norms or articulating their position on aspects of international law.

The cyber norms explained

4. The 11 agreed norms are primarily about promoting interstate cooperation, protecting critical infrastructure, safeguarding global supply chains, providing assistance when required, respecting human rights and privacy, and preventing the malicious use of digital technologies in states' national territories. Three of the norms involve actions that countries should avoid, and the other eight are actions that states should encourage.

- <u>Limiting norms:</u>

  i. States should not knowingly allow their territory to be used for internationally wrongful acts using information and communications technologies (ICTs)

  ii. States should not conduct, or knowingly support, ICT activity that intentionally damages critical infrastructure.

  iii. States should not conduct, or knowingly support, activity to harm the information systems of another state's emergency response teams (CERTs/CSIRTs) and should not use their own teams for malicious international activity.

- <u>Positive norms:</u>

  iv. States should cooperate to increase stability and security in the use of ICTs and to prevent harmful practices.

  v. States should consider all relevant information in case of ICT incidents.

  vi. States should consider how best to cooperate to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs.

  vii. States should take appropriate measures to protect their critical infrastructure.

  viii. States should respond to appropriate requests for assistance by other states whose critical infrastructure is subject to malicious ICT acts.

  ix. States should encourage responsible reporting of ICT vulnerabilities and should share remedies to these.

x. States should take steps to ensure supply chain security, and should seek to prevent the proliferation of malicious ICT and the use of harmful hidden functions.

xi. States should respect the UN resolutions that are linked to human rights on the internet and to the right to privacy in the digital age.

5. Following their adoption by the General Assembly, these norms have been endorsed by other bodies, including the Group of Seven (G7), the Group of 20 (G20), and the Association of Southeast Asian Nations (ASEAN).

The norms in practice

6. Examples of potential breaches (noting that the specific circumstances of a situation would determine whether it actually constitutes a breach of norms, or indeed international law) include:
   - A state which knowingly tolerated malicious non-state actors operating from within its borders to conduct attacks against another country's nuclear reactor, resulting in serious damage and loss of life, could be a breach of norm (i).
   - A piece of malware used by one state to shut down another state's power, telecommunications, transportation, or financial systems could constitute a breach of norm (ii) ("critical infrastructure" is not defined – it is left for states to determine themselves).
   - A state which deliberately hid or ignored credible information that computer hardware was being developed and sold with malware pre-installed could be breaching norms (ix) and (x).

7. On the other hand, there is a range of malicious activity that would not necessarily constitute a breach of the norms. That does not make the behaviour inherently acceptable, rather it just indicates that there is not currently international consensus that it crosses a line. This might include, for instance:
   - A state conducting massive and untargeted espionage against another government.
   - A state undertaking cyber compromises for the indiscriminate theft of private citizens' personal identifiable information.
   - A state sharing or publishing information about a cyber vulnerability for the purposes of widespread exploitation of those vulnerabilities by other malicious actors.

Commitments prohibiting espionage for commercial advantage

8. In addition to the 11 agreed norms, there are several multilateral commitments focused on prohibiting state-sponsored cyber-enabled economic espionage and intellectual property theft for commercial gain:
   - In 2015, G20 leaders agreed that "no country should conduct or support ICT-enabled theft of intellectual property, including state secrets or other confidential business information, with the intent of providing competitive advantages to companies or the commercial sector."
   - All APEC economies agreed in the 2016 Leaders' Declaration that they should not "conduct or support ICT-enabled theft of intellectual property or other confidential business information, with the intent of providing competitive advantages to companies and commercial sectors."

9. A number of bilateral agreements also exist in this space, many involving China. In 2015, the US and China signed a bilateral agreement that included the commitment that neither the US nor Chinese government would knowingly conduct or support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, for commercial advantage. The UK and Australia also have similar bilateral commitments with China.

10. These commitments (and subsequent condemnation of breaches of these commitments) indicate a norm prohibiting this commercial cyber espionage exists, or is taking shape.

Other norms

11. A range of parallel norm-building efforts has emerged alongside the UN processes. Whilst these other efforts are legitimate attempts to further build the normative framework to guide state behaviour in cyberspace, these are arguably less widely accepted s6(a) than the 11 agreed in a UN context.

12. Nevertheless, the overlapping nature of these regimes (and the involvement of non-state actors in the development of those noted below) mean they can be complementary and mutually-reinforcing. Examples include:

- **The Freedom Online Coalition** (FOC)'s Free and Secure Recommendations, a set of 13 "normative" recommendations designed to raise the profile of human rights as an integral consideration in cybersecurity policymaking, were developed by a multi-stakeholder group and endorsed by FOC member governments (including New Zealand).
- **The Global Commission on the Stability of Cyberspace** (GCSC), a multi-stakeholder initiative involving 26 experts from a range of fields (New Zealand is not represented), which has put forward a framework, principles, and eight norms to help foster responsible state and non-state behaviour in cyberspace.
- **The Paris Call for Trust and Security in Cyberspace**, initiated by France and endorsed by a range of states, including New Zealand, and other entities (including the private sector, civil society academics, and technical experts). The Call affirmed the importance of norms for cybersecurity.
- **Private sector initiatives** such as Microsoft's Cybersecurity Tech Accord, Siemens's Charter of Trust, and Kaspersky Lab's Global Transparency initiative. These industry-led norms lay out voluntary measures that private actors agree to take to protect cyberspace, and their users and customers from cyber threats while using their products and services.

The current situation and challenges

13. Despite the UN membership's endorsement of the Framework of Responsible State Behaviour in Cyberspace and the norms therein, the global discussion on these issues remains contentious, and implementation and evolution of the Framework is challenging.

Implementation and accountability

14. Although these have been endorsed by all UN member states, the 11 norms need to be strengthened and brought to life through enforcement and accountability – otherwise they risk becoming meaningless if states do not implement them, and hold each other to account for failure to adhere to them. Silence in the face of breaches risks their erosion, which in turn risks contributing to a new de facto norm — "anything goes" — which increases the risks to international peace, security and stability.

15. s6(a)

s6(a) [redacted]

16. There are various efforts underway to support the strengthening and consistent implementation of these norms including: efforts by the UN Open Ended Working Group (OEWG) to develop guidance on implementation and a checklist of steps countries should take to implement them; states' outreach and capacity-building (both with other states and civil society/the private sector) to support better understanding of the norms and their application; and the absorption of norms into national strategies, and bilateral or multilateral agreements.

17. Further, there are efforts to hold states to account for violating the norms. This primarily occurs through public attribution statements, which seek to "name and shame" the state responsible for the malicious activity, and which might specifically mention the norm(s) breached. Whilst these attributions are unlikely to stop such breaches, the public articulation, attribution, and condemnation of certain behaviour helps determine and reinforce the lines of what is acceptable and unacceptable – which, crucially, may also have an impact on third countries' behaviour.

18. Alongside attribution statements, there are other measures states may take to deter malicious cyber activity – such as pursuing criminal charges against individual members of state-sponsored groups responsible for malicious activity, or implementing sanctions – which can contribute to the normative framework by demonstrating where behaviour is considered unacceptable.

The development of new norms

19. Both the UN Group of Governmental Experts (GGE) and the OEWG have recognised that there may be a need to develop new norms in the future. However, this too is a contentious issue. Some states consider the current set of norms sufficient, and others (including New Zealand) have argued that – until there is compliance with current norms – we should not seek agreement on further ones. Officials have concerns that opening up discussions on new norms will detract from efforts to implement and hold to the existing ones.

20. At the same time, officials recognise there are some areas where malicious state-sponsored activity seems to be increasing or evolving, and which may warrant actions (including attribution statements) to deter and respond to such behaviour.

21. For instance, recent international statements (including by New Zealand) condemning the SolarWinds compromise and attributing the activity to Russian state actors highlight that at least some in the international community consider this unacceptable behaviour. s6(a) [redacted]

[redacted]

- s6(a)

23. Additional concerns exist around other activity which is not strictly counter-normative but which is nevertheless concerning (as noted in paragraph 7), such as indiscriminate collection of personal identifiable information, or activity which is highly disruptive and costly to the private sector.

24. There are currently no formal moves to develop new norms relating to these issues in either the UN or other contexts. However, consistent state practice in expressing concern about such issues could over time result in the development of norms against this type of behaviour, even in the absence of intentional actions or explicit agreement in a multilateral or multi-stakeholder context.

Recommendations

25. It is recommended that you note the contents of this aide-memoire.

	NOTED
Tony Lynch Deputy Chief Executive, National Security Group Department of the Prime Minister and Cabinet	Rt Hon Jacinda Ardern Prime Minister and Minister for National Security and Intelligence
Date: / / 2021	Date: / / 2021

DEPARTMENT OF THE PRIME MINISTER AND CABINET
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

Aide-Memoire

NATIONAL SECURITY ISSUES OF DDOS ATTACKS DURING LOCKDOWN

To	**Rt Hon Jacinda Ardern, Minister of National Security and Intelligence**	**Report No**	2122NSP/025
From	Tony Lynch, Deputy Chief Executive, Department of the Prime Minister and Cabinet	**Date**	16/09/2021

Purpose

1. This note provides a brief overview of the implications for national security of Distributed Denial of Services (DDoS) attacks occurring during lockdown conditions.

Comment

DDoS attacks are a staple of cybercrime

2. DDoS attacks are a long-established form of cyber attack. While their general nature remains the same – overwhelming an internet connected system with data – the techniques used in these attacks have evolved to make them more potent. While mitigations exist, the way the internet deals with data means it is unlikely this form of attack will cease to be a significant threat in the foreseeable future (a brief description of DDoS is attached as Appendix One).

3. The recent DDoS attacks targeting domestic organisations are within the expected range of the scale and type of cybercrime activity that will affect New Zealand. DDoS attacks against financial institutions are reported to have increased since 2020. s6(a)

4. The sophistication of the most recent DDoS attacks demonstrate the continuing increase in capability among malicious actors. Recent attacks here and overseas have shown increased ability of actors to work around mitigations and to ramp up the sheer scale of attacks. s6(a)

Lockdowns may incentivise DDoS

5. It is possible that New Zealand organisations are currently being targeted due to cyber criminals assuming that organisations are less able to mitigate attacks during lockdown, with IT staff out of the office, and that the impacts of disruption will be greater with increased remote working and online commerce. There are no strong indicators, however, that this is the case in recent attacks.

6. While financial gain is the primary driver of cyber criminals there are a wide range of motivations for carrying out DDoS attacks, including notoriety and state-sponsored interference in other nations' affairs. The actors undertaking DDoS attacks often react to media attention and mitigation efforts to pressure organisations to pay a ransom or gain insights into defenders' responses.

…while lockdowns and the wider COVID-19 response may also alter the impact of DDoS attacks

7. The COVID response, and lockdowns in particular, makes internet connectivity relatively more important and DDoS attacks relatively more impactful. The main reasons for greater impact include:

    a. Greater collateral damage as the disruption to home internet connections meant many more organisations had staff unable to work than would normally be the case. For example the disruption to the Vocus network, on 3 September;

    b. Ongoing crisis response increases the chance that network downtime will occur at a critical time. s6(a) [redacted]

    c. Organisations that may be restricted from providing goods and services physically during lockdown will be more severely affected by internet disruptions than they would normally.

…and these impacts highlight some general resilience issues

8. DDoS attacks involve internet traffic management which is managed by private sector organisations. DDoS mitigation is best addressed by organisations working with their service providers, ISPs and security firms, who are well placed to implement technical responses. Cyber security awareness, technical literacy and cost are the primary barriers to these measures being in place. Government should therefore continue to promote good cyber security practices and the importance of business contingency planning.

9. Ensuring that critical services are not dependent on infrastructure with single points of failure, or have alternative forms of provision, is vital to maintaining security and wellbeing. Ongoing crises such as COVID-19 create an inherent concurrency issue for potential national security threats and we must continue to plan for managing responses in the face of multiple disruptions.

10. The Minister Responsible for the Government Communications Security Bureau and the Minister for the Digital Economy and Communications will be reporting back to Cabinet in March 2022 with options to improve protection of nationally significant organisations and incentivise cyber resilience overall [CBC-21-MIN-0086refers]. The impact of DDoS attacks will be considered as part of this work.

NOTED

Rt Hon Jacinda Ardern
Minister of National Security and Intelligence

Date: / /

Tony Lynch
Deputy Chief Executive, Department of the Prime Minister and Cabinet

Appendix One:

WHAT IS A DISTRIBUTED DENIAL OF SERVICE?

A denial of service attack is designed to overwhelm websites by generating excessive volumes of web requests, for the purpose of stopping, or limiting, any genuine web browser requests for the website. When the requests are coming from multiple sources it is a *Distributed* Denial of Service (DDoS).

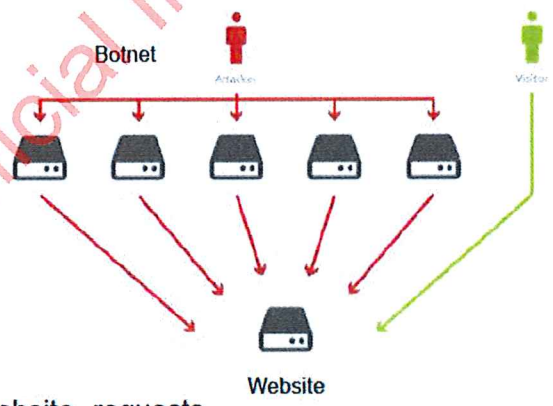
Is a DDoS an attack?

There are many instances where websites become overwhelmed and stop working (ticket booking sites for a popular show, for example). While these are not usually termed a DDoS, effectively it is the same. In the physical world it would be like a flash mob preventing entry to a building.

When the intent is malicious, the DDoS is usually termed a 'DDoS attack'. This attack does not involve exploiting any unpatched vulnerabilities as the DDoS requests look like normal web requests (just more of them).

What creates the excess volume of website requests?

Cybercriminals control armies of compromised computers and network devices, sometimes numbering in the tens of thousands, and distributed across the world. This is called a botnet. Using a botnet to direct millions of website requests to a target website results in overwhelming the website.



What can be done?

Stopping a DDoS attack is difficult, as separating out genuine and non-genuine website requests is not usually possible. The most effective mitigation is to enable the website to handle a greater number of requests, enabling the website to handle both the genuine and non-genuine requests at the same time.

Alternatively, identifying the controllers of the botnet and compelling them to stop the attack may be possible.

Has New Zealand cyber defence failed to protect victims of DDoS?

It's important to note that victims of DDoS attacks have not been compromised by malware. Instead, the victims don't have the infrastructure or systems in place to simply and quickly scale up to handle the increase in web request volumes.

There are several commercial vendors that specialise in providing DDoS mitigation services. The mitigations are usually large-scale networks that are able to balance the load across multiple webservers and locations.

DEPARTMENT OF THE PRIME MINISTER AND CABINET
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

Briefing

MEETING WITH FACEBOOK REPRESENTATIVES - 28 SEPTEMBER 2021

To **Minister for the Digital Economy and Communications and Commerce and Consumer Affairs** (Hon Dr David Clark)			
Date	27/09/2021	**Priority**	Routine
Deadline	27/09/2021	**Briefing Number**	2122NSP/034

Purpose

This brief provides you talking points and background ahead of your meeting with Facebook representatives on 28 September 2021. We expect the meeting will cover COVID-19 misinformation, the Digital Strategy for Aotearoa, encryption, the Digital Identity Trust Framework, the Consumer Data Right, privacy and ethics.

Recommendations

1. **Note** the contents of this briefing

Tony Lynch **Deputy Chief Executive** **National Security Group**	Hon Dr David Clark **Minister for the Digital Economy and Communications and Commerce and Consumer Affairs**
27/09/2021	...../...../....

Contact for telephone discussion if required:

Name	Position	Telephone	1st contact
Halia Haddad	Acting Manager National Cyber Policy Office	s9(2)(a)	✓
s6(a)	Principal Policy Advisor National Cyber Policy Office		

Minister's office comments:

- ☐ Noted
- ☐ Seen
- ☐ Approved
- ☐ Needs change
- ☐ Withdrawn
- ☐ Not seen by Minister
- ☐ Overtaken by events
- ☐ Referred to

MEETING WITH FACEBOOK REPRESENTATIVES - 28 SEPTEMBER 2021

Introduction

1. You are meeting with Facebook representatives s9(2)(a) on 28 September 2021 from 4:15pm to 5:00pm.

2. You met s9(2)(a) previously, on 3 June 2021, and discussed how Facebook can dock into the Digital Strategy, and its moves towards end-to-end encryption across its messaging services.

3. Facebook continues to be one of the most popular social media platforms in New Zealand, with almost three quarters of the population being active users.[1]

4. We expect the main topics to discuss with s9(2)(a) include:
   a) COVID-19 misinformation
   b) Encryption
   c) Digital Strategy
   d) Digital Identity Trust Framework / the Consumer Data Right
   e) Privacy and ethics
   f) Online scam awareness

Talking points

5. The talking points below are included at the start of the briefing to focus on the headlines for each topic. More background is included for each topic from page 6.

General

- Thank you for reaching out – we appreciate the constructive engagement.
- I understand that Facebook is engaging with officials on issues including the Christchurch Call, CERT NZ's Cyber Smart Week, the Digital Boost Alliance and encryption.

Christchurch Call

- I'd like to express my gratitude for the constructive and collaborative spirit with which Facebook has approached the Christchurch Call
- The response from the tech sector to the Christchurch Call has underscored the importance of constructive relationships between government and industry.
- Facebook has also been involved in our domestic conversation on countering violent extremism online, led by the Department of Internal Affairs. We will continue to work closely with you and digital industry on ensuring our domestic systems and regulation are fit for purpose.

[1] https://gs.statcounter.com/social-media-stats/all/new-zealand

COVID-19 and misinformation

- Thank you for the positive cooperation offered to a range of agencies involved in our COVID-19 response.
- This remains a pressing concern for government. We appreciate the work you have done in reducing the spread of COVID misinformation through de-amplification, post deletion and temporary bans.
- We have also appreciated the amplification of our official COVID communication campaign and look forward to working with you as this continues to evolve.
- Mis- and disinformation is not going to disappear. It is important that we build on this relationship to address the more difficult aspects, such as algorithms and processes that amplify harmful material. It is only through a multi-stakeholder approach, engaging government, civil society, online service providers and others, that we will be able to mitigate the worst effects of mis- and disinformation

Encryption and content regulation

- I am aware of Facebook's plans to consolidate, and provide end to end encryption, on its messaging services.
- New Zealand acknowledges the privacy drivers for this. We are also concerned that unless workable solutions are developed, this could reduce ours and Facebook's ability to protect citizens from harm.
- Can you update me on Facebook's work and thinking in this area?
- New Zealand remains committed to working constructively, collaboratively, and creatively with Facebook on safety issues in end-to-end encrypted environments .
- s9(2)(ba)(i)
- s9(2)(g)(i)

Digital strategy

- The Digital Strategy for Aotearoa is being released at the end of this month. It will be our blueprint for a higher productivity, lower emissions future where all New Zealanders can flourish in a digital world.
- We know that, for people and businesses to embrace digital technology, they need to trust and be confident in how these technologies are created, used, and governed, so openness and transparency will be key to the Strategy.
- Our intention is for this to be a living strategy that continues to evolve and change with technology, ensuring that we can adapt to new issues and opportunities.

- We hope that the Digital Strategy will put in place the right foundations to enable New Zealand to be a world leading digital nation built on trust and known for the ethical deployment of emerging technologies.

- We are grateful for your membership of the Digital Boost Alliance that amplifies our efforts to drive productivity, wellbeing, and social inclusion in a way that benefits everyone.

- What are the 'compliance requirements' that prevent Facebook from making advertising credits available to the private small business trainees (as a way to start their social media advertising) involved in the Digital Boost programme, when Facebook regularly provides such credits to small businesses directly?

Digital identity

- It is important that people trust the way their identity data is handled and know how their data is being used.

- The upcoming Digital Identity Services Trust Framework is a regulatory regime that will promote the provision of secure, adaptable and trusted digital identity services in Aotearoa.

- We are working towards international mutual recognition of our digital identity trust frameworks, which is the critical first step to full interoperability.

- The Digital Identity Services Trust Framework Bill will be introduced to Parliament this year. We are developing the Trust Framework rules that accredited participants will need to meet. The prerequisites for accreditation are being developed and will be the subject of stakeholder engagement.

- As a member of the Digital Identity Alliance, what are your priorities for the future of handling identity data?

Consumer Data Right

- You're probably aware the Government has agreed to establish a Consumer Data Right framework for New Zealand.
- I'd be interested in any views you might have on Australia's implementation of the Consumer Data Right. Do you see any lessons New Zealand can draw from Australia's experience so far?
- My officials at MBIE are continuing to engage with interested parties as part of the CDR policy process and would be happy to engage with Facebook that would be useful.

Privacy and ethics

- Facebook has received a lot of criticism regarding privacy since 2018. I note it has also progressed user control of privacy settings since 2018, which I understand was driven both by Europe's strict privacy laws but also compliance action taken against Facebook.
- What is unique to Facebook with letting users take control of their privacy settings that other social media platforms do not do?
- New Zealand updated its privacy legislation in December last year, with the Privacy Act 2020. This Act allows the Privacy Commissioner to take more direct action against agencies that breach New Zealand's privacy laws.

- How will Facebook work with the Office of the Privacy Commissioner to ensure New Zealanders' personal information is safe and secure and that Facebook acts in accordance with our privacy law?
- **Trust** is one of the three pillars for the Digital Strategy for Aotearoa I announced earlier this year. How does Facebook plan to build, maintain and grow New Zealanders' trust in Facebook services?
- I am concerned about the use of facial recognition technology in New Zealand, following an academic report released in December last year that proposed legal and ethical frameworks for the use of this technology.
- As Facebook has the ability to tag users in other's photos using facial recognition technology, what settings, controls and assurances can Facebook provide that this technology is used appropriately?
- I would be interested to hear what improvements Facebook is implementing to mitigate and prevent divisive content that impacts the mental health of teens in New Zealand.

Online scam awareness

- We look forward to your collaboration with CERT NZ on your campaign to promote awareness of online scams and to extend audience reach during CERT NZ's Cyber Smart Week commencing on 18 October 2021.
- This important collaboration supports our efforts to build a culture where New Zealanders can operate securely online

Background

COVID-19 and misinformation

6. COVID-19 misinformation is spread in New Zealand through multiple channels, including social and traditional media (television, radio and print), pamphlets, posters and letterbox drops, and word of mouth.

7. As the global vaccine roll out began, CERT NZ became aware of cyber criminals using public interest in the vaccine to scam individuals out of money or personal information. CERT NZ, DPMC, and the Ministry of Health (MoH) identified the need for a single mis/disinformation reporting point for the public.

8. To simplify reporting lines, CERT NZ agreed to collect reports and pass them to the relevant authority. This coordination role is part of work by all government agencies to support the Unite against COVID-19 effort.

9. CERT NZ requested that New Zealanders submit reports of vaccine scams, so advice could be provided to the public on how to avoid them. New Zealanders also started to report what they thought to be misinformation or disinformation.

10. CERT NZ does not determine if reports contain misinformation or disinformation. It refers reports to agencies with relevant subject matter expertise, such MoH or DPMC, to determine accuracy and inform strategic or public awareness work.

11. A weekly summary of COVID-19 scam and mis/disinformation reports is also shared with other government agencies. This approach has demonstrated the benefits of a central reporting point for understanding volume, impact. and development of public messaging.

Social media and dissemination of COVID-19 misinformation

12. Social media platforms (e.g. Facebook, YouTube, Twitter, Telegram etc.) are the most common means of disseminating and amplifying vaccine misinformation and disinformation, often with international reach.

13. Vaccine-related misinformation on social media can include:

    a) Rumours on social media about 'consequences' of the vaccine, which can be spread by those who think it is genuine, out of interest or concern.

    b) Misinformation about certain treatments or medicines designed to look like genuine medical advice.

    c) Mask-wearing conspiracies that are not underpinned by science.

14. Facebook has taken some positive steps to reduce the spread of COVID misinformation using existing tools, such as de-amplification, post deletion and temporary bans. Through DPMC's COVID-19 Group, DIA and the Ministry of Health (with the Chief Censor and NetSafe) we have established positive working relationships s9(2)(a) to flag issues. We work closely with Facebook to remove harmful content and ensure the visibility of our official COVID communications campaign.

15. More can be done by social media companies such as Facebook to address algorithms that can promote and amplify mis- and disinformation. The response from Facebook, and the tech sector more generally, to the Christchurch Call has underscored the importance of building constructive relationships between government and industry. s9(2)(g)(i)

16. Governmental work takes a whole-of-society, multi-stakeholder approach to strengthening resilience to mis- and disinformation. Government, civil society, tech companies, media, academia, business and the public all have a role to play in ensuring public safety.

Encryption and content regulation

Privacy First Policy

17. In 2019 Facebook revealed its Privacy First Policy and integration of Facebook Messenger, Instagram, and WhatsApp to create an interoperable, end-to-end encrypted (E2EE) messaging system.

18. E2EE is a method to secure communications and uses encryption to exclude third parties from accessing content shared between communicating users. Policy making around safety and security in encrypted environments has proved highly contentious since encryption began to be widely used in the 1990s. The advent of E2EE last decade was greeted with a similar mixture of concern for online safety and advocacy of encryption as a tool to protect security and privacy.

19. In December 2019, the UK, Australia and USA issued an open letter expressing concern at Facebook's E2EE proposals, asking Facebook not to proceed without including a means for lawful access to the content of communications. Facebook published an open response saying it hoped to work with governments on solutions that keep people safe and their communications private. Facebook also emphasised the privacy, security and user safety benefits of encryption, confirming it would not compromise user privacy by building in "back doors". A wide range (over 100) of civil society organisations, including InternetNZ, also published an open letter to Facebook in support of the move to E2EE.

20. The UK published a follow-up statement in April 2020 urging technology companies, including Facebook, to embed public safety in system designs, to allow companies to act against illegal content on their platforms, and to enable law enforcement access to content. New Zealand supported the statement alongside a broad coalition of like-minded jurisdictions (see Briefing 1920NSP/066).

21. s9(2)(ba)(i)

Impact of E2EE on child sexual abuse material and cybercrime

22. When E2EE is enabled on Messenger (as it already is on WhatsApp) Facebook will be unable to directly access user content. This will make it more difficult to identify and prevent serious crimes and online harm through content moderation.

23. A specific concern raised in the April 2020 statement was the impact of E2EE on investigating child sexual abuse material (CSAM). Reporting of CSAM is a statutory requirement for US service providers through the US National Center for Missing and Exploited Children (NCMEC). Facebook presently uses photo-matching technology to match known CSAM with content on its servers.

24. If Facebook implements E2EE it will be unable to monitor CSAM images through its current photo-matching technology. This is a concern because the vast majority of the NCMEC referrals come from Facebook (20.3 million out of a total of 21.4 million reports in 2020). Facebook removes approximately 8 million CSAM images from its servers every three months and accounts for a significant proportion of referrals sent to New Zealand authorities.

25. Facebook has stated it wishes to work on solutions that could enable it to mitigate safety risks. Solutions suggested include the use of Artificial Intelligence, machine learning tools to assess harmful behaviour from user data and disclosure to law enforcement of the metadata, or "*outside the envelope*" information, such as sender and receiver identification, IP address, basic subscriber information, date, time, and location data.

26. We understand the Apple announcement on 6 August 2021 to introduce new child safety features for US users to detect CSAM through on-device machine learning s9(2)(g)(i)

Apple has since decided to take additional time to consider and make improvements to its proposed child safety features. We understand Apple's announcement has been greeted with concern by some other providers, given that Apple's absence of engagement with

privacy and security advocates beforehand led to a backlash against the proposals and their subsequent postponement.

s9(2)(ba)(i)

[redacted]

Digital Strategy for Aotearoa

30. Our tech sector is the fastest growing industry in New Zealand and has grown 30 per cent faster than the economy overall. This sector offers us scope to foster a resilient, diversified and future focused economy.

31. The Digital Strategy for Aotearoa is being released at the end of this month. It will be our blueprint for a higher productivity, lower emissions future where New Zealanders have the opportunity to flourish in a digital world. Digital offers the opportunity for New Zealand to make a step change, by reducing our historical challenges of being small in scale and distant from major global markets, which have held back our economic development and prosperity.

32. The Digital Strategy consists of three key themes:
    a) Mahi tika (trust) – Building the right foundations so that Aotearoa New Zealand can lead the world
    b) Mahi tahi (inclusion) – Making sure all New Zealanders can ride the digital wave
    c) Mahi ake (growth) – Leveraging what makes New Zealand unique

33. There will be a series of virtual hui in October to start the conversation with New Zealanders on what they think is important for New Zealand's digital future. This includes making sure tangata whenua contribute to decisions about how we create the Strategy and the actions we take as a result, so that the Digital Strategy reflects Te Ao Māori and embodies Te Tiriti o Waitangi – the Treaty of Waitangi.

Digital Boost Alliance

34. Facebook is a member of the Digital Boost Alliance and has committed to:
    a) Providing scholarships to small business professionals to upskill in Facebook Professional Certifications

b) Providing free digital skills education to small businesses both virtually and in person across cities and towns New Zealand through the Boost with Facebook programme
c) Partnering with local organisations focussed on expanding the economic empowerment opportunities for Māori owned businesses

35. Facebook advises its 'compliance requirements' prevents it from making advertising credits available to the small business trainees (to start their social media advertising) involved in the Government's Digital Boost programme. We are aware Facebook regularly provides such credits to small businesses directly. s9(2)(g)(i)

Digital identity

36. It is important people know and trust the way their identity data is handled and used. Providing people with greater control over their identity data will help build and maintain trust.

37. The upcoming Digital Identity Services Trust Framework is a regulatory regime that will promote the provision of secure, adaptable and trusted digital identity services in Aotearoa. The Trust Framework will complement the development of the Consumer Data Right (see below), by enabling people to securely access and share their personal information digitally.

38. The Digital Identity Services Trust Framework Bill will be introduced to Parliament this year. s9(2)(f)(iv)

39. Key partners such as Australia and the United Kingdom are modernising their digital identity systems and are taking a similar approach to New Zealand. We are working towards international mutual recognition of our digital identity trust frameworks, which is the critical first step to full interoperability.

40. We have not recently engaged with Facebook about the Digital Identity Trust Framework. However, Facebook has expressed an interest in digital identity internationally.

41. With approximately two billion users worldwide, Facebook has the potential to be a significant participant in the international digital identity market. In August 2021, Facebook joined the Digital Identity Alliance, which is a global private public partnership focused on the future of digital identity.

Consumer Data Right

42. In July, the Government agreed to establish a legislative framework for a Consumer Data Right (CDR). This will give consumers the ability to request data held about them be shared with trusted third parties. MBIE officials are considering further aspects of the CDR, including institutional arrangements and the compliance and enforcement regime, with a view to introducing legislation to Parliament in mid-2022. The legislative framework will be designed to apply to the entire New Zealand economy and gradually deployed on a sector-by-sector basis.

43. This approach is broadly like that in Australia, where the banking sector is implementing the CDR, and the energy and telecommunications sectors will follow. Digital platforms are a potential priority sector for further roll-out of the CDR in Australia.

44. s9(2)(g)(i), s9(2)(b)(ii)

Privacy

Cambridge Analytica

45. Facebook has progressed privacy and ethics considerably since the events following the 2018 revelations that Facebook had shared data from potentially over 87 million profiles (including an estimated 64,000 profiles from New Zealanders)[2] to Cambridge Analytica without the user's knowledge or consent. This information was used to create micro-targeting advertisements for the 2016 presidential campaigns for Senator Ted Cruz and President Donald Trump. Facebook was fined by the Federal Trade Commission (FTC) for these activities and it agreed to pay a fine to the US Securities and Exchange Commission for misleading investors about the misuse of user's profiles and data.

Privacy programme and privacy controls

46. In April 2018 Facebook announced that its global operations would follow the European Union's stringent General Data Protection Regulations (GDPR). GDPR has requirements that are more stringent than the protections and rights in New Zealand's Privacy Acts of 1993 and 2020.

The key elements of Facebook's privacy programme include:

a) Implementing a governance structure that incorporates an independent Privacy Committee of their Board.
b) Rebuilding the new privacy program from the ground up in consultation with experts.
c) Standing up and continuing to grow a central privacy organisation.
d) Developing new teams and processes to assess and mitigate risk, including a dedicated Privacy Review function to evaluate potential privacy risks posed by new or modified products or data practices.

47. As part of an agreement between Facebook and the FTC, a qualified, independent Assessor produces regular reports on the effectiveness of Facebook implementation and maintenance of their privacy programme. Several necessary improvements were identified in the Assessor's first report, including enhancing the central privacy organisation's oversight role, and bolstering privacy safeguards and controls using technology that builds on core strengths in automation and analytics.

48. Facebook gives users control over their privacy settings and claims to be transparent about how personal information is collected and used. Users can edit settings, including revoking permission for apps to continue accessing personal data and disable the ability for Facebook to run facial recognition algorithms on photos of users. Criticism remains that many of these settings are enabled by default and there are many settings.

[2] "Facebook notification of New Zealanders impacted by Cambridge Analytica breach", 9 April 2018, https://www.privacy.org.nz/publications/statements-media-releases/facebook-notification-of-new-zealanders-impacted-by-cambridge-analytica-breach/

The Facebook Files – Wall Street Journal

49. A series of Wall Street Journal articles published in mid-September 2021 based on internal Facebook documents describes how the company has created separate content moderation rules for VIP users, the negative effect of the company's Instagram platform on teen mental health, and how the company's tweaks to its algorithms have resulted in more divisive content on Facebook. Taken together, the articles contradict the company's public statements regarding rules governing content and their enforcement, its claims about its products' impact on user health, and the stated goals of algorithm tweaks.

50. The US Senate commerce subcommittee on consumer protection has announced plans to investigate Facebook over its knowledge of Instagram's impact on teens.

Facebook in New Zealand

51. The Office of the Privacy Commissioner named Facebook critically in its 2018 Annual Report, which it does to incentivise organisations' compliance with the Privacy Act. This followed Facebook's refusal to cooperate with an investigation into their compliance with the Privacy Act, as Facebook believed it operated under Irish GDPR laws and was thus not subject to New Zealand's Privacy Act. The Privacy Commissioner clarified that as it operates in New Zealand Facebook is subject to New Zealand privacy laws. Facebook continued to not comply.[3]

52. The Privacy Commissioner further criticised Facebook following the terrorist attack on the Christchurch masjidain of 15 March 2019, which was broadcast live on Facebook, noting that Facebook did not commit to any changes to its Facebook Live technology.

The Office of the Privacy Commissioner (OPC) was asked to provide advice, as an independent regulator, for your meeting and provided paragraphs 52-57:

53. "The Privacy Act 2020 applies to Facebook in relation to Facebook's handling of personal information when it undertakes business in New Zealand and provides services to New Zealanders. This is the case regardless of where Facebook's offices are located, or where it collects, holds or processes personal information relating to its business activities in New Zealand.

54. The Privacy Act is very clear about the Act's extra-territorial application, as a result of a deliberate reform to privacy legislation for the protection of New Zealand consumers. Clarification of the Act's application to overseas agencies brought it into line with comparable privacy laws, including Australia's.

55. OPC's previous engagement with Facebook under the Privacy Act 1993 was unsatisfactory, as Facebook declined to recognise the Privacy Commissioner's jurisdiction. While the Privacy Act has now been strengthened, s9(2)(g)(i)

[redacted]

[3] "Privacy Commissioner Annual Report 2018" and "Privacy Commissioner: Facebook must comply with NZ Privacy Act", 28 March 2018, https://www.privacy.org.nz/publications/statements-media-releases/privacy-commissioner-facebook-must-comply-with-nz-privacy-act/

56. Similar jurisdictional issues have arisen in other countries. In 2020, Facebook opposed service of pecuniary penalty proceedings by the Australian privacy regulator, claiming it did not carry on business in Australia.

57. As a global company, Facebook is subject to varying privacy regimes in different jurisdictions, and this can create enforcement challenges for regulators. OPC works with privacy regulators in other jurisdictions on facilitating enforceability and promoting compatibility of privacy laws across borders.

58. OPC has advocated for changes to the Privacy Act that would bring New Zealand law more into line with globally leading privacy regimes like the GDPR. These changes would also provide OPC with more effective tools for regulating powerful transnational entities such as Facebook. Changes to the Privacy Act recommended by the Privacy Commissioner, but which the Government has not yet agreed to implement, include:
    a) a right to data portability (which may be implemented, at least partially, through current work on a consumer data right)
    b) a right to erasure in appropriate cases, so that individuals can require the deletion of personal information about them that is inaccurate, misleading or out of date
    c) requirements for algorithmic transparency in appropriate cases
    d) an ability for the Privacy Commissioner to apply to the courts for civil penalties of up to $1 million to be imposed for serious or repeated breaches of the Privacy Act (in line with the NZ Commerce Commission and the Australian privacy regulator)."

Online scam awareness

59. The recently published New Zealand Crime and Victims Survey (NZCVS) incorporates statistics on cybercrime and fraud (or scams). It is estimated that during 2019/2020 8.3% of adults (342,000 adults) had been victims of scams. However, 93% of all scams were not reported to the Police. Factors for failing to report include victim embarrassment and a lack of understanding if a crime has been committed.

60. Facebook is collaborating with CERT NZ, NetSafe and NZ Police on a campaign to promote awareness of online scams. The six topics covered are fake prizes and promotions, online shopping scams, romance scams, phishing, investment, and impersonation. The main aim of the videos is to raise awareness of the scams, so people know to avoid them.

61. The campaign will start at the beginning of October and run for approximately five weeks. It will be promoted through digital advertising on Facebook and Instagram, plus billboards. The campaign will overlap in part with CERT NZ's Cyber Smart Week campaign commencing 18 October 2021.

Consultation

62. DPMC consulted NZ Police, Department of Internal Affairs, Ministry of Business, Innovation and Employment, Office of the Privacy Commissioner and CERT NZ in preparing this brief.

Attachments:		
Attachment A:	Biographies	Withheld in full under section 9(2)(a) of the Act

DEPARTMENT OF THE PRIME MINISTER AND CABINET
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

Briefing

RESPONSE TO LETTER FROM THE SPEAKER OF THE HOUSE OF REPRESENTATIVES ON CLOUD SERVICES

To
Minister of National Security and Intelligence (Rt Hon Jacinda Ardern)
Minister Responsible for the GCSB (Hon Andrew Little)
Minister for the Digital Economy and Communications (Hon Dr David Clark)

Date	30/09/2021	**Priority**	Routine
Deadline	15/10/2021	**Briefing Number**	2122NSP/011

Purpose

To provide a draft response to a letter from the Speaker of the House of Representatives on the potential use of Cloud services by the Parliamentary Service, including background and advice on several specific questions raised by the Speaker.

Recommendations

1. **Note** that the Speaker has sought Ministers' opinion on the potential rollout of Cloud-based tools for the Parliamentary Service, including that some Members' information may be stored s6a before migrating to the onshore Microsoft data centre region.
2. **Note** that Cloud services offer increased functionality, security and cost-effectiveness, but carry some jurisdictional and sovereignty risks that cannot be fully mitigated.
3. In responding to the Speaker, **request** a briefing on the Parliamentary Service's risk assessment, including on risks relating to Ministerial data and proposed mitigations, prior to decisions on Cloud adoption. **YES / NO**
4. **Sign** the letter at Attachment A. **YES / NO**

Tony Lynch **Deputy Chief Executive** **National Security Group** **Department of the Prime Minister and Cabinet**	Rt Hon Jacinda Ardern **Minister of National Security and Intelligence**
29/09/2021	…../…../….
Hon Andrew Little **Minister Responsible for the GCSB**	Hon Dr David Clark **Minister for the Digital Economy and Communications**
…../…../….	…../…../….

Contact for telephone discussion if required:

Name	Position	Telephone		1st contact
Halia Haddad	Acting Manager, National Cyber Policy Office	DDI s9(2)(a)	Mobile	✓
s6(a)	Principal Policy Advisor, National Cyber Policy Office	DDI	Mobile s9(2)(a)	

Minister's office comments:

- ☐ Noted
- ☐ Seen
- ☐ Approved
- ☐ Needs change
- ☐ Withdrawn
- ☐ Not seen by Minister
- ☐ Overtaken by events
- ☐ Referred to

RESPONSE TO LETTER FROM THE SPEAKER OF THE HOUSE OF REPRESENTATIVES ON CLOUD SERVICES

Purpose

1. The Speaker of the House of Representatives has written to seek your views on a possible Parliamentary Service move to Cloud services (Attachment A). This paper provides considerations to inform Ministers' response to the letter. A draft response to the Speaker is included for your consideration (Attachment B).

Cloud services provide significant benefits

2. The usability of the current Parliamentary Information and Communications Technology (ICT) toolset is a source of frustration for users. This can hinder productivity and increase security risk, especially if staff use work arounds and turn to 'shadow Cloud' services.

3. COVID has shown the benefits of Cloud for the public service and New Zealanders more broadly, delivering resilience, continuity, and agility in enabling secure online working and collaboration from home. Our digital economy is increasingly turning to hyperscale Cloud to operate and sustain businesses, and as a platform for local and global growth.

4. Additionally, Cloud adoption is a way of improving government security swiftly and at scale and is a key cyber protection measure in the 0increasingly sophisticated threat landscape. Cloud adoption is therefore an important part of our digital economy, digital public service and cyber security plans.

5. Finally, the External Independent Review on Bullying and Harassment in the New Zealand Parliamentary Workplace recommended Parliamentary Service and the Department of Internal Affairs consider how best to provide staff with better tools to support flexible working, including ICT systems and devices. Officials assess that a move to Cloud-based tools would assist with meeting that recommendation.

There are risks associated with Cloud services

Security

6. Cloud services are designed to be highly secure and are routinely updated and improved by Cloud providers. The effective management of Cloud services requires specialist skills and knowledge. Where these are lacking, security issues may arise. Cloud security risks are most often realised due to misconfiguration or administrator inexperience with Cloud systems.

7. Officials would encourage the Parliamentary Service to use the New Zealand Information Security Manual (NZISM) Azure Blueprint for their relevant Microsoft Cloud infrastructure. This blueprint provides a means of easily and quickly implementing, and maintaining, NZISM-compliant Cloud infrastructure for Azure services. s6a

s6a

s9(2)(ba)(i)

Jurisdictional risk

9. In the context of Cloud services, jurisdictional risks occur where data is subject to the laws of other countries in which Cloud service providers may store, process, or transmit data. Jurisdictional risks may lead to situations incompatible with New Zealand law or that prejudice our national interests. We have included in Attachment C a synopsis on jurisdictional risk.

10. At present, New Zealand does not have local hyperscale Cloud data centres for large data storage. Most Cloud services used by New Zealand agencies are currently based s6(a) Microsoft and AWS are building data centres to host Cloud services in New Zealand. Microsoft's new data centre region is expected to be operational in early to mid-2023. AWS' facilities are expected to begin operations shortly after this. Other Cloud service providers (Spark/CCL, DCI, Canberra Data Centres, Datagrid) have also expanded, announced plans and/or begun construction of New Zealand facilities.

11. s6(a) and s9(2)(f)(iv) s6(a)

12. If the Parliamentary Service implemented other Cloud tools, data could also be stored in other jurisdictions and subject to relevant laws in those jurisdictions. Engagement with the providers of such Cloud tools will be necessary to understand where data is transferred, stored, and processed, and to assess the relevant laws to understand jurisdictional risks.

What is special about data held by the Parliamentary Service?

s6a

14. The Parliamentary Service was invited by Cabinet to follow the NZISM and guidance on adoption of Cloud technologies. The NZISM notes that the majority of jurisdictional, sovereignty and privacy risks cannot be wholly and completely managed with controls available today. The agency head or Chief Executive must therefore carefully consider

those risks before adopting Cloud services as, ultimately, it is the responsibility of agencies to assess risks and determine whether they should accept them.

15. Under the Government's Cloud First policy, to move to Cloud services agencies must:

    a) Make Cloud adoption decisions on a case-by-case basis following a risk assessment; and

    b) Only store data classified at restricted or below in a Cloud service, whether it is hosted onshore or offshore.

s9(2)(f)(iv)

s9(2)(f)(iv)

Māori Data

18. Parliamentary Service holdings are likely to include Māori data. Members may wish to seek advice and assurance from the Parliamentary Service in respect of the implications of Cloud adoption for Māori data held by the Parliamentary Service.

19. We recommend the Parliamentary Service engages with its Te Tiriti partners to work through the specific risks and mitigations associated with Māori data. To support this engagement, the Parliamentary Service may wish to draw on existing frameworks and tools, for example:

    a) Archives New Zealand has produced guidance in setting its approach to management of data in its archival management system that references data location and specific data of interest to iwi/Māori;[1] and
    b) Stats NZ applied a privacy impact assessment framework while assessing whether to migrate certain systems (excluding the Integrated Data Infrastructure - IDI) to Microsoft Office 365 hosted on infrastructure located in Australia, including drawing upon applicable dimensions of the Ngā Tikanga Paihere guidelines.[2]

s9(2)(f)(iv)

[1] Refer to "Cloud Services: Information and records management considerations", available at https://archives.govt.nz/manage-information/how-to-manage-your-information/digital/cloud-services
[2] Available at https://data.govt.nz/toolkit/data-ethics/nga-tikanga-paihere/

22. For instance, if the Parliamentary Service decides to offer Microsoft 365, there would be significant benefits to users from collaboration tools beyond traditional productivity tools such as Word, PowerPoint and Excel. Microsoft 365 provides capabilities for collaboration, data analytics, process automation and more.

Conclusion

23. A draft response to the Speaker's letter is enclosed for your consideration reflecting the points discussed above.

Consultation

24. This briefing was prepared by DPMC with input from DIA, GCSB and a letter from Minister Little of 8 July 2021.

Attachments:	
Attachment A:	Letter from the Speaker
Attachment B:	Draft response to the Speaker
Attachment C:	Jurisdictional risk synopsis

ATTACHMENT A

Letter from the Speaker

IN CONFIDENCE

Office of the Speaker of the House of Representatives

Rt Hon Jacinda Ardern
Prime Minister

Hon Andrew Little
Minister for Government Communications Security Bureau, and the New Zealand Security Intelligence Service

Hon David Clark
Minister for Digital Economy and Communication

Cloud Services for Parliament

1. This paper sets out a possible Parliamentary Service approach to move to Cloud services and the impact and mitigating actions of members of Parliament and Minister's information as a result of it, and seeks your views.

Background

2. Cabinet endorsed the Government Cloud Acceleration Programme in 2016 (SEC-16-MIN-0026).

3. The Parliamentary Service cooperates with Government initiatives and guidance when it aligns with best practice and does not compromise Parliament's traditional independence from the Government.

4. Current guidance from the Government Chief Digital Officer (GCDO) for organisations requires use public cloud services in preference to traditional IT systems on a 'case-by-case basis, following risk assessments.' As a relatively small entity, the Parliamentary Service recognises there are many benefits that public cloud services provide its users, including ease-of-use, value for money, improved security, and improved choice.

5. In late 2018, the Parliamentary Service suspended its migration to cloud-based productivity tools (Microsoft 365) because of concerns about political and jurisdictional risk posed by the offshore hosting of member emails, as well as perceived limitations on Parliamentary Privilege. Following the decision to suspend that project, the Service also stopped or significantly slowed adoption of other cloud solutions for a time.

6. The Parliamentary Service IT group has continued to work with internal stakeholders, supported by the GCDO, to better quantify and understand the risks and benefits that cloud solutions pose for parliament. It has also met with senior members of other government agencies, including the Ministry of Defence, to understand their approach to managing the risks associated with cloud solutions. They have successfully applied the GCDO's Cloud Risk Assessment framework and information security patterns within Parliamentary Service.

7. Since mid-2018 the Service successfully implemented several cloud based solutions, including the successful roll out of Zoom videoconferencing for members and staff at the

beginning of the COVID-19 lockdown. The cloud services adopted to date have focused primarily on non-Parliamentary or corporate use cases, such as health and safety reporting and customer service management, where risks to Members and Ministers is not a significant factor..

8. In November 2020, I gave approval for a small non-government party and its members to use cloud-based productivity tools (Microsoft 365).

9. In January 2021 the Parliamentary Service Chief Executive and the Clerk of the House of Representatives approved a new rollout of cloud-based productivity tools for core Service Corporate and Office of the Clerk staff respectively. Members, Ministers, and their support staff are currently out of scope of this initiative.

10. There are increasing requests from other parties and members for the rollout of these services to be made widely available.

11. The Parliamentary Service has found it increasingly difficult and costly to deliver required capabilities only on-premises over the past two years. Technology vendors are rapidly shifting investment to cloud products and retiring support for legacy on-premises versions.

12. The Service is currently developing a roadmap to align rollout of cloud-based tools to members, Ministers, and their support staff.

13. The Service will continue to implement public cloud services where are they deliver features that Members, Ministers, and their staff need, where they deliver improved security and value for money, and where they do not introduce significant political, security, or jurisdictional risks to Parliament or its Members.

14. While initially some of the members' information would be stored in the offshore facility in Australia, the Service will migrate that information to the onshore Microsoft availability zone, which is currently under construction, as soon as it is launched.

Recommendations

I recommend that you:

1. **Provide your opinion** on the current development by the Service of a roadmap to align rollout of cloud-based tools to members, Ministers, and their support staff.

2. **Provide your opinion** about the fact that while initially some of the members' information may be stored in the offshore facility s6a the Service will migrate that information to the onshore Microsoft availability zone, which is currently under construction, as soon as it is launched.

3. **Note** that industry investment trends toward cloud-only solutions will, over time, increase the difficulty to identify new suitable on-premises solutions and increase the cost and risk of maintaining existing, legacy on-premises solutions.

Rt Hon Trevor Mallard
Speaker of the House of Representatives

ATTACHMENT B

Draft response to the Speaker

Dear Speaker,

Thank you for your letter of 21 June. We welcome the opportunity to make suggestions on the development of a roadmap for use of Cloud-based tools by the Parliamentary Service.

Capability considerations

It is important that the Parliamentary Service provides capable and secure ICT tools to Ministers, Members of Parliament and support staff.

The obsolescence of the non-Cloud Parliamentary toolset is a source of tremendous frustration for Members and staff (as encapsulated in Recommendation 58 of the Francis Review). Inadequate work tools hamper productivity but also introduce external security risks, for example when individuals have little choice but to use non-approved apps to get work done.

Better productivity, collaboration and mobility can only be achieved through adoption of Cloud services and should occur as soon as is safely possible.

Cloud security considerations

We agree that the decision to suspend the migration to Cloud-based productivity tools (specifically Microsoft 365) in 2018 was appropriate given the uncertainty around jurisdictional risks.

The Parliamentary Service was invited by Cabinet to follow the New Zealand Information Security Manual (NZISM) and guidance on adoption of Cloud technologies. The NZISM notes that jurisdictional, sovereignty, and privacy risks cannot be wholly and completely managed with the controls available today. Therefore, they should be carefully considered and accepted by the agency head or Chief Executive before the adoption of such Cloud services.

s9(2)(f)(iv) [redacted]

s6(a) and s9(2)(f)(iv) [redacted]

s6(a) and s9(2)(f)(iv)

Māori data governance

The Parliamentary Service holdings are likely to include Māori data. Members may wish to seek advice and assurance from the Parliamentary Service in respect of the implications of Cloud adoption for Māori data. We recommend that the Parliamentary Service engage with its Te Tiriti partners to work through the risks and mitigations and refer to existing frameworks and tools used by Stats NZ and Archives New Zealand.

s9(2)(f)(iv)

In summary

s9(2)(f)(iv)

Yours sincerely,

Rt Hon Jacinda Ardern

Minister of National Security and Intelligence

Hon Andrew Little

Minister Responsible for the GCSB

Hon Dr David Clark

Minister for the Digital Economy and Communications